## GUIDANCE ON SECURITY REQUIREMENTS SCHEDULE SECTIONS APPLICABILITY

**The Security Schedule sets out the technical requirements underpinning the security of BAT's global networks and systems. References in this guidance to BAT include each entity within the BAT Group.**

The Security Schedule should be included in any Supplier contract where the Suppliers' process and / or store BAT information and / or has access to BAT environments and/or the Supplier's services are classified as critical for continuity of BAT's operations per the **GUIDANCE ON SECURITY REQUIREMENTS SCHEDULE SECTIONS APPLICABILITY**. Only the relevant sections are to be included into the Supplier contract taking into account the relationship risk level and service profile and scope. Cyber risk score in Coupa RA AFC workflow supports identification of level and type of cyber risk of a relationship. When you are involved in such Supplier contracts, please work together with local LEX and local IDT and the relevant business area to ensure this Security Schedule is included in the contract as applicable.

1. **Where the Supplier does not access BAT IT/OT networks, systems, physical or logical assets (in each case whether owned or used by BAT), does not access, process, or store BAT data, or the Supplier is not classified as critical to continuity of BAT operations**, confirmed by Cyber Triaging output in Coupa RA reporting Low Risk, none of the sections of the Schedule apply.

2. **Where the Supplier is not providing BAT with IT related services and is not accessing BAT IT/OT networks, systems, physical or logical assets (in each case whether owned or used by BAT), does not access, process, or store BAT data,** but is however is classified as critical for BAT continuity of operations (which will only be the case where service / goods provided to BAT have critical dependency on the Supplier's own IT continuity and potential incidents may not be fully compensated with business continuity plans), apply the following sections of this schedule:
   - section 1: General Security Requirements
   - section 2: Security Incidents Notification and Response

3. **Where the Supplier is not providing IT related services to BAT but is accessing BAT IT IT/OT environment or assets, but not granted with privileged or administrator type of access,** apply the following sections of this schedule:
   - section 1: General Security Requirements
   - section 2: Security Incidents Notification and Response

4. **Where the Supplier is not providing to BAT with IT related services but is accessing or processing BAT Most Confidential or Confidential information, including Personally Identifiable Information classified by BAT,** apply following sections of this schedule:
   - section 1: General Security Requirements
   - section 2: Security Incidents Notification and Response.

5. **Where the Supplier is providing BAT with IT related services** and will have as part of the service access to BAT environment and/or BAT data then the below sections apply based on type of IT Service:.

| | TYPE OF IT SERVICE | APPLICABLE REQUIREMENTS |
|---|---|---|
| | All IT Services | • **Section 1**: General Security Requirements<br>• **Section 2**: Security Incidents Notification and Response |
| | IT Services based on **infrastructure or cloud services** (except SaaS) | • **Section 1**: General Security Requirements<br>• **Section 2**: Security Incidents Notification and Response<br>• **Section 3**: Infrastructure or cloud-based services requirements |
| | IT Services **based on SaaS** | • **Section 1**: General Security Requirements<br>• **Section 2**: Security Incidents Notification and Response<br>• **Section 4**: Security requirements for SaaS |

| | | |
|---|---|---|
| | **IT Development services** | • **Section 1**: General Security Requirements<br>• **Section 2**: Security Incidents Notification and Response<br>• **Section 5**: Security requirements for Development |
| | All other types of IT services like application administration, help desk, consulting etc. | • **Section 1**: General Security Requirements<br>• **Section 2**: Security Incidents Notification and Response |

Security requirements should anticipate maximum scope of services and/or access including potential for future extensions to avoid BAT needing to renegotiate the terms of the contract in the event of increased cyber security requirements due to enlarged scope of services.

For any proof of concept (**PoC**) projects, the assessment as to which sections in this Schedule are applicable to any PoC should be based on the PoC scope and purposes only. Cyber risk assessment should be repeated post PoC for potential future Supplier services in production environments.

**SCHEDULE [XX]**
**SECURITY REQUIREMENTS**

1.In this Schedule [xx] (Security Requirements) the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

(a) **["Agreement"** means [insert reference to the relevant services agreement to avoid having to amend the reference to "Agreement" throughout the schedule should your contract or template use a different reference] [(including all SOWs (if any)) forming part thereof])];

(b) "**Anomalies and Events"** irregular or unusual activity which is a deviation from the norm and/or any activity inconsistent with the expected norm;

(c) **"Audit Right Holder"** [has the meaning given to it in [insert] ]/ [means BAT and each of its Affiliates, BAT Audit Representatives and Regulatory Authorities acting in accordance with their regulatory or supervisory powers;

(d) **"BAT Audit Representative [**has the meaning given to it in [insert]] /[ representatives of any member of BAT Group (including its internal auditors), its appointed consultants, external auditors and their appointed consultants and any other auditors, regulators, inspectors or consultants any member of BAT Group may designate as "BAT Audit Representatives" in writing from time to time;]

(e) "**BAT Confidential Information"** has the meaning given to it in [insert]/[means Confidential Information of any member of the BAT Group which is disclosed to or otherwise learnt by the Supplier or any Contractor in connection with this Agreement (or its subject matter)];

(f) **"BAT Cybersecurity Procedure"** means the BAT's cybersecurity procedure [available at {insert website} at the Commencement Date] / [in Appendix xx] as amended, varied or updated by BAT from time to time [pursuant to the Change Control Procedure]/ [and the Supplier shall comply with all such amendments, variations, or updates from the date on which the amended, varied or updated **BAT Cybersecurity Procedure** is made available on BAT's website or is otherwise notified to the Supplier;

(g) "**BAT Data**" [has the meaning given to it in [insert] / [means all data or records of whatever nature and in whatever form relating to the BAT Group's business, its or their operations, facilities, assets, employees or otherwise relating to the business of BAT or any member of BAT Group from time to time, whether such data subsisted before the commencement of this Agreement or was created or processed as part of, or in connection with, the ***Services*** and including any **BAT Confidential Information** and BAT Personal Data;

(h) "**BAT Environment**" means any networks and network devices, server hardware, storage systems, computer systems, applications, software or software components used by BAT and/or any of its Affiliates from time to time (including any systems used by BAT and/or any of its Affiliates with which any Supplier system shall connect, exchange data, interface or otherwise interoperate or communicate);

(i) **"BAT Group Company"** [has the meaning given to it in [insert]] [means each entity within the BAT Group, and **BAT Group Companies** shall be construed accordingly;

(j) "**BAT Personal Data**" has the meaning given to it in **Schedule xx (Data Protection)**;

(k) **"Best Industry Practice"** [has the meaning given to it in [insert]] / [means all relevant practices and professional standards (including without limitation (ISO 27001, NIST, CIS ) and the exercise of that degree of skill, care, diligence, prudence, foresight and operating practice which, at the relevant time, would reasonably and ordinarily be expected of a reputable, skilled, experienced and [market-leading] expert service provider performing services substantially similar to the Services (taking into account factors such as the service levels, term and pricing) and having regard to the consensus of professional opinion on security and the Risks to security that may apply from time to time, to customers of the same nature and size as the BAT Group]**;**

(l) **"Commencement Date"** [has the meaning given to it in [insert clause] of the Agreement]/ [means [insert date];

(m) **"Contractor"** [has the meaning given to it in [insert]/[means any third party from time to time providing goods (and for this purpose the term "goods" includes software) and/or services to the Supplier in connection with this Agreement and includes any sub-contractor, contractor or agent of the Supplier of any tier, any of the Supplier and any sub-contractor, contractor or agent of any tier of any such Affiliate

(n) "**Data Protection Laws**"[ has the meaning given to it in [insert]] [***[to be defined per Agreement / by End Market locally. For EEA End Markets please defer to Centre's definition]];***

(o) "**DevSecOps"** means software development related services, including based on any Agile / SCRUM and DevOps frameworks, where new software solutions are created or changes to existing ones are introduced;

(p) ["**Group Acceptable Use of Technology Procedure**" means the BAT's Group Acceptable Use of Technology Procedure [available at {insert browser address} at the Commencement Date] / [in Appendix xx], as amended, varied or updated by BAT from time to time [pursuant to the [Change Control Procedure/ [and the Supplier shall comply with all such amendments, variations, or updates from the date on which the amended, varied or updated **Group Acceptable Use of Technology Procedure** is made available on BAT's website or is otherwise notified to the Supplier];

(q) **["Regulatory Authority"** [has the meaning given in [insert]/[any governmental or regulatory authority or other competent authority or entity in any jurisdiction responsible for regulating or supervising BAT or any member of the BAT Group];

(r) **["Related Persons"** [has the meaning given to it in [insert]] / [means, in relation to a Party, that Party's Affiliates, that Party's and/or its Affiliates' employees, officers, shareholders, representatives, agents, consultants, contractors, permitted licensees of any tier (including sub-licensees), suppliers and advisers including, in the case of BAT, [BAT Service Providers] and [BAT Audit Representatives], but shall exclude the other Party and that other Party's Affiliates];

(s) "**Resilience**" means the ability to prepare for and adapt to changing conditions, and to withstand and recover rapidly from Risks. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents affecting or with the potential to affect Security;

(t) "**Risk**" means any reasonably identifiable circumstance or event having a potential adverse effect;

(u) "**Security Event**" an event that may have an impact on operations (including mission, capabilities, or reputation) and/or the Security of Systems or any BAT Data and/or that impacts or may impact the confidentiality, integrity or availability of any BAT Data;

(v) "**Security Incident**" means any event having an actual adverse effect on Security;

(w) "**Security**" means the state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured;

(x) "**Services**" has the meaning given to it in [insert clause] of the Agreement;

(y) "**Supplier**" means [xx]; [insert reference to the supplier to avoid having to amend the reference to "Supplier" throughout the schedule should your contract or template use a different reference];

(z) "**Supplier Personnel**" means [insert]/[has the meaning given to it in [insert clause] of the Agreement];

(aa)"**Systems**" means the computing environment, communications environment, and / or information and records environment (consisting of, but not limited to, hardware, software, network and information systems, paper and / or other physical records), data or premises that may be used by the Supplier and/or any Contractor or (as the context requires) BAT and/or any of its Affiliates in connection with its provision of Services. References in this Schedule to the "Supplier's System" are to Systems that may be used by the Supplier and/or any Contractor and include Systems owned by or licensed to the Supplier and/or any Contractor. References in this Schedule to "BAT Systems" are to Systems that may be used by one or more BAT Group Companies and include Systems owned by or licensed to one or more BAT Group Companies.

(bb)"**Term**" has the meaning given to it in [insert]/[means the period during which this Agreement is in full force and effect as provided by the terms of this Agreement];

In this Schedule, the words "other", "includes", "including" "for example" and "in particular" do not limit the generality of any preceding words and any words which follow them shall not be construed as being limited in scope to the same class as the preceding words where a wider construction is possible.

References in this Schedule to "BAT assets" include physical and logical assets that may be owned or used by one or more BAT Group Companies.

**[Without prejudice to the foregoing, this Schedule shall be deemed incorporated into Appendix 2 to the Data Transfer Clauses as defined in Schedule xx (Data Protection) where all references to Supplier shall be construed as the 'data importer' and all references to BAT shall be construed as the 'data exporter'.]**

## SECTION 1: GENERAL SECURITY REQUIREMENTS

### 1. General Security Requirements

#### 1.1. Security Requirements

(a) The Supplier shall (i) adhere to the technical and organisational security measures set out in this Schedule which shall be reflected in its information security policies; and (ii) perform the Services in accordance with Best Industry Practice including without limitation as it relates to cyber security, protection of any BAT Data or BAT assets that might be impacted by actions of the Supplier or any Contractor.

(b) The Supplier confirms that at the date of the Agreement it has and shall continue to have in place such technical and organisational measures as may be required to manage the Risks posed to the Security of BAT Systems and BAT assets (where Supplier has access to BAT Systems or BAT's physical or logical assets in connection with the Agreement) and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement), including in accordance with Data Protection Laws, including such measures as would be considered appropriate by the consensus of professional security opinion, having regard to the state of the art.

(c) The Supplier shall take appropriate and proportionate measures to prevent and minimise the impact of Security Incidents affecting the provision of the Services, with a view to ensuring the protection of BAT Data and BAT Environment as well as continuity of services provided to each BAT Group Company.

(d) Without prejudice to paragraphs 1.1.(b) and 1.1.(c) above, the Supplier shall (at its own cost):

i. implement such technical and organisational measures to manage the Risks to BAT Data and BAT Systems as may be notified to it by BAT in writing from time to time, in accordance with Best Industry Practice;

ii. review the level of compliance and effectiveness of the technical and organisational measures it has implemented on an annual basis (or unless agreed otherwise between the Parties), and undertake such updates, enhancements or remediation work as may be reasonably required to comply with the Agreement, provided that it shall not make any changes that might result in a lesser degree of protection being afforded to any affected system related to the provision of Services;

iii. maintain and comply with widely accepted cybersecurity frameworks that are appropriate to establish effective security practices and manage risk in accordance with Best Industry Practice.

(e) Where the Supplier has access to BAT Systems or any BAT assets (whether physical or logical) in connection with the Agreement, in addition to the Supplier's other obligations in the Agreement, the Supplier shall (and shall procure that the [Supplier Personnel] and [Contractors] shall) comply with the [BAT Cybersecurity Procedure] [and the Group Acceptable

Use of Technology Procedure] and the Supplier shall perform Services in accordance with the aforementioned BAT policies and procedures.

(f) With regard to the maintenance and compliance with widely accepted cybersecurity frameworks that are appropriate to establish effective security practices and manage risk in accordance with Best Industry Practice as required under paragraph 1.1 (d)(iii), , Best Industry Practice is deemed to include compliance with widely accepted cybersecurity frameworks including without limitation Trust Criteria confirmed by SOC2 Type 2 Report or alternatively ISO 27001 and ISO27002 or NIST CSF with NIST SP800-53 and in each case verified through an independent compliance assessment with certification of such compliance. The Supplier shall at all times maintain and comply with such certifications and provide evidence of them to BAT upon its request. Related assessments (e.g., SOC 2 Type 2 Report or ISO 27001 Certification) must cover all geographical locations and entities providing services to BAT and/or any of its Affiliates, the full scope of these services, as well as the controls performed by the Supplier and/or any Contractor which are likely to impact the internal controls of BAT and/or any of its Affiliates.

(g) The Supplier shall ensure that sites owned, controlled or used by the Supplier or any Contractor where any BAT Data is stored (where the Supplier and/or any Contractor is or are holding any BAT Data on the Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement), including data centres, offices, and off-site storage facilities, will have appropriate logical and physical security controls in accordance and in line with Best Industry Security Practice.

**1.2 Identifying Risks to Security**

1.2.1 The Supplier shall ensure:

(a) it has an adequate understanding of its organisation to manage Risks to Security, including but not limited to, Risks to the Supplier's Systems, BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement), people, assets, and the Services;

(b) there is an organisation-wide approach to managing Risks to Security that uses risk-informed policies, processes, and procedures to address potential Security Events;

(c) threats to the Security of the Supplier's Systems and any BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement), both internal and external, are identified and documented;

(d) the relationship between Risks to Security and delivery of the Services is clearly understood and considered when making decisions, which may affect the Security of the Supplier's Systems and any BAT Data;

(c) its security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination), processes, and procedures are maintained and used to manage the protection of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement). This will include, but is not limited to ensuring that:

i. cyber and information security policies are established and communicated;
ii. cyber and information security roles and responsibilities are coordinated and aligned with internal roles and external partners;
iii. legal and regulatory requirements regarding cyber and information security, including privacy, data protection and civil liberties obligations, are understood and managed;
iv. governance and risk management processes address Risks to Security;

v. a process to identify, assess and manage supply chain risks is established, implemented and maintained. This will include, but is not limited to ensuring that:
    a. supply chain risk management processes are identified, established, assessed and managed to reduce Risks to Security;
    b. suppliers and third-party partners of the Supplier's Systems, components of such Systems, and services are identified, prioritized, and assessed using a supply chain risk assessment process;
vi. a baseline configuration of information technology and control systems is created and maintained incorporating security principles and Best Industry Practice (e.g. concept of least functionality);
vii. a System development life cycle to manage the Supplier's Systems is implemented and maintained;
viii. response and recovery planning and testing are conducted with Suppliers and third-party providers;
ix. there are clear standards on how to implement and assess that the Supplier's infrastructure and sites where any BAT Data is transmitted and stored, including data centres, offices, and off-site storage facilities, have the appropriate logical and physical security controls in line with Best Industry Practice and verified by independent assessment as set out in paragraph 1.1(f).

(d) a vulnerability management plan is developed and implemented;

(e) Risks caused by System vulnerabilities are identified, documented and addressed;

(f) it receives, generates, and reviews prioritised information that informs continuous analysis of Risks to Security as the threat and technology landscapes evolve, including the collection and use of cyber and information security threat intelligence from information sharing forums and other sources;

(g) it uses real-time information to understand and consistently act upon information security supply chain risks associated with the products and services it provides and that it uses.

(h) there is a process of continuous improvement, including but not limited to, incorporating current Security technologies and practices to respond to Risks to Security;

(i) that BAT Data, personnel and all Systems that enable the delivery of the Services are identified and managed consistently with their relative importance to the Security of Systems and BAT Data. This should include, but is not limited to ensuring that:

(i) cyber and information security roles and responsibilities for the entire Supplier workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established;

(ii) dependencies and critical functions for delivery of the Services are established;

(iii) Software platforms and applications within the organization are inventoried;

(iv) organisational communication and data flows are mapped;

(v) external information Systems of the Supplier are catalogued;

(vi) resources (e.g., hardware, devices, data, time, personnel, and software) are prioritised based on their classification and criticality to the Services and protection of the Supplier's Systems, BAT Systems (to the extent specified in the Services) and BAT Data;

(vii) Resilience requirements to support delivery of the Services are established for all operating states (e.g., under duress/attack, during recovery, normal operations);

(j) it communicates proactively, using formal and informal mechanisms to reduce Risks to Security emanating from third parties in its supply chain. This will include, but is not limited to ensuring that:
(i) contracts with suppliers and third-party partners are used to implement appropriate technical and organisational measures to reduce Risks to Security; and

(ii) Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting the requirements under this Schedule. SSAE16/ISAE 3402, SSAE18 (SOC 2 Type 2), ISO 27001 audit and other Best Industry Practice and security certification frameworks (to the extent that maintenance of them and compliance with them is required under this Schedule) must be assessed.

**1.3 Protecting Systems and BAT Data**

1.4.1 The Supplier shall ensure:

(a) it develops, implements and maintains appropriate technical and organisational measures to protect the Supplier's Systems, BAT Systems (to the extent specified in the Services), BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement) and the delivery of the Services;

(b) it limits or contains the impact of a potential Security Event on Systems, BAT Systems (to the extent specified in the Services), BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement) and the risks to rights and freedoms of data subjects;

(c) the Supplier's Systems are managed effectively to reduce Risks to Security and protect the confidentiality, integrity, and availability of BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement). This will include, but is not limited to ensuring that:

(i) Data-in-transit is protected (Secure Transport Protocols TLS v1.2 at minimum);

(ii) the Supplier's Systems are formally managed throughout removal, transfers, and disposition activities;

(iii) adequate capacity is maintained to ensure availability of the Supplier's Systems and BAT Data;

(iv) protections are implemented and maintained to prevent data leaks;

(v) integrity checking mechanisms are used to verify software, firmware, and information integrity;

(vi) separate databases will be maintained for different types of BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement) ;

(vii) paper, equipment, media and data is disposed of securely;

(viii) it enters into a confidentiality agreement (on no less onerous terms than those contained in clause xx (Confidentiality)) with each person, contractor or other third party accessing any BAT Data or BAT Systems whereby each such person, contractor and third party is bound by obligations [owed to and enforceable by the Supplier and each BAT Group Company] that are equivalent to those imposed on the Supplier under clause xx (Confidentiality) as if such person, contractor or third party were the Supplier; and

(ix) integrity checking mechanisms are used to verify hardware integrity;

(f) maintenance and repairs of the Supplier's Systems and components of such Systems do not affect the Security of those Systems or any BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement). This will include ensuring that:

(i) development and testing environment(s) are separate from the production environment;

(ii) maintenance and repair of organisational assets are performed and logged, with Supplier approved and controlled tools;

(iii) remote maintenance of the Supplier's Systems is approved, logged, and performed in a manner that prevents unauthorised access; and

(iv) if any BAT Data is disposed of, such disposal takes places in a secure manner such that the BAT Data is not recoverable;

(g) technical security solutions are managed to ensure the Security and Resilience of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement). This will include, but is not limited to ensuring that:

(i) removable media is protected, and its use restricted according to Best Industry Practice;

(ii) all the Supplier's Systems have secure configuration;

(iii) all laptop and desktop PC hard drives are encrypted according to Best Industry Practice;

(iv) ensuring mobile device management software is used to administer security controls on corporate supplied and employee owned devices used for business purposes, if any BAT Data will be accessed on the device;

(v) applications and programming interfaces (APIs) are designed, developed, deployed, and tested in accordance with Best Industry Practice and Secure Software Development Methodology (SSDLC) standards, for example OWASP;

(vi) unless agreed otherwise between the Supplier and BAT, regarding any weakness exposed as a result of a penetration test to the Supplier's Systems, the Supplier must notify BAT promptly and then the following shall apply:

- if a critical, high or a medium risk weakness has been detected in a live environment during the processing of any BAT Data (as determined by BAT), then remediation must be complete no longer than two weeks after the weakness has been detected;
- if a low risk weakness has been detected in a live environment during the processing of any BAT Data (as determined by BAT) then remediation must be complete within two months.

**1.4 Security Awareness**

1.5.1 The Supplier shall ensure its personnel and partners are provided with Security awareness education and are trained to perform their Security-related duties and responsibilities in a way which is consistent with Best Industry Practice. This will include, but is not limited to ensuring that:

(a) all personnel undergo industry standard background checks following good hiring practices;

(b) all users of the Supplier's Systems and BAT Systems (where Supplier has access to BAT Systems or BAT physical or logical assets in connection with the Agreement) and/or any BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement) are informed of Risks to Security and trained appropriately (in any event awareness training shall be conducted on an annual basis) to reduce those Risks.

(c) privileged users understand their roles and responsibilities in relation to the Security of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement), including but not limited to, their responsibilities regarding protection of their user account and password details;

(d) all personnel are trained in the secure handling and care of BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement);

(e) third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities in relation to the Security of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement);

(f) senior executives understand their roles and responsibilities in relation to the Security of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement); and

(g) physical, cyber and information security personnel understand their roles and responsibilities in relation to the Security of the Supplier's Systems and BAT Data (where the Supplier and/or any Contractor is or are holding any BAT Data on Supplier's System or where any BAT Data is accessed or processed by or on behalf of the Supplier and/or any Contractor in connection with the Agreement).

**1.5 Third Party Audit**

(a) On the Commencement Date, and on an annual basis (during the Term [and during the period in which the Supplier is obliged to provide any agreed termination assistance]), the Supplier shall provide to BAT from an independent and reputable auditor, a SOC 2 Type 2 report (**SOC 2 Report)**, covering the full scope of the Services and where relevant addressing the impact on the BAT Environment or the BAT Group including any elements of the Services performed by the Contractors or any other third parties on behalf of the Supplier. The Supplier shall make the Supplier staff reasonably available for follow up questions on the SOC 2 Report.

(b) Where the **SOC 2 Report** highlights exceptions, the Supplier shall promptly (and in any event no later than 30 days from the **SOC 2 Report** highlighting the exceptions), provide to BAT additionally to the report also a remediation plan to address such exceptions. Where the Supplier fails to address and remedy any exceptions raised in the reports to the reasonable satisfaction of BAT within a reasonable period, then this shall constitute a material breach of this Agreement that is incapable of remedy and BAT shall have the right to terminate this Agreement for material breach by giving notice in writing to the Supplier.

(c) The Supplier shall provide BAT with ongoing access to the reports referred to in this paragraph 1.5. For the avoidance of doubt, the Supplier shall bear any costs incurred by it in complying with this paragraph 1.5 including in respect of engaging an independent and reputable auditor.

**1.6 Cross default**

1.6.1 Any material breach of this Schedule by the Supplier shall constitute a material breach of the Agreement.

**1.7 Subcontractors and personnel**

1.7.1 An obligation on the Supplier to do, or refrain from doing, any act or thing shall include an obligation upon the Supplier to procure that the [Supplier Personnel] and [Contractors] also do, or refrain from doing, such act or thing, and the Supplier shall be liable for the acts and omissions of the Supplier Personnel and Contractors as if they were its own acts or omissions.

1.7.2 The Supplier shall not sub-contract any of its rights and obligations under this Agreement unless in accordance with the Agreement. The Supplier shall impose contractual obligations on each sub-contractor that are no less onerous than those contained in this Schedule. BAT's consent to the Supplier sub-contracting or delegating the performance of any of its obligations under the Agreement which may be granted under the Agreement, will not relieve the Supplier of any of its obligations to BAT under this Agreement. BAT may require the Supplier to cease using a subcontractor if the subcontractor a commits a material breach of this Schedule.

**1.8 Indemnity**

1.8.1 The Supplier shall, during the Term and thereafter, indemnify and hold harmless each member of BAT Group (and their respective successors and assigns) in respect of any and all [Losses] incurred or suffered by or made against any of them (wholly or partially) resulting directly or indirectly from, or connected in any way with, any of the matters listed below, whether or not such Losses were foreseeable at the date of entering this Agreement:

(a) the breach by the Supplier or any member of the Supplier Group of any obligations under or in connection with this Schedule including all amounts paid or payable by BAT or any Related Persons to a third party which would not have been paid or payable if the Supplier's breach had not occurred;

(b) any act or omission of any individual, who is or was a member of Supplier Personnel, facilitated or enabled through any access to any network, device, system(s), hardware, or software used by any BAT Group Company where the Supplier would have been liable for the act or omission had it been its own or where the access has not been authorised by BAT or has been granted in reliance on inaccurate, incomplete or out of date information provided by or on behalf of the Supplier in respect of Supplier Personnel.

1.8.2 Nothing in this Agreement shall limit or exclude the liability of the Supplier for any Losses for which the Supplier provides an indemnity under this paragraph 1.8.

**1.9 Audit Rights**

1.9.1 In addition to the other audits permitted under the Agreement, during the Term, [during any period in which any [Statement of Work] is in effect, and during the period in which the Supplier is obliged to provide termination assistance], the Audit Right Holders shall have the right to audit Supplier's IT security controls on reasonable notice (which shall be no less than 30 days prior to the date of the audit unless a shorter period is required by the relevant Regulatory Authority or the audit is requested in circumstances of suspected fraud or circumstances where there has been an actual or suspected breach, Security Event or Security Incident) and the Supplier shall allow such audit to take place. Subject to paragraph 1.9.7 below**Error! Reference source not found.**, such requests shall not exceed more than one (1) in any 12-month period.

1.9.2 In responding to any audit conducted pursuant to paragraph 1.9.1, the Supplier will demonstrate or provide BAT with documentation that sufficiently evidences the Supplier's compliance with IT security requirements (or a higher security level where applicable) (including the Supplier's ISO 27001 & 27002 certification, SOC2 Type2 assessment report and a high-level summary of vulnerability tests). The Supplier may provide reports that contain sensitive information pertaining to the Supplier's environment (including vulnerability scanning) in a redacted format (that is to say in a format where the Supplier has removed any information that could potentially lead to a security breach if disclosed). The Supplier must ensure that it provides a remediation plan to BAT for any open high risks and conduct risk assessments in respect of any such open high risks on a periodic basis and in any event at least annually. BAT will treat all records discussed pursuant to any audit conducted under this Schedule in accordance with clause [xx](Confidentiality).

1.9.3 For the purpose of facilitating an audit under this paragraph 1.10 the Supplier shall provide to any of the Audit Right Holders (at no cost to BAT):

(a) reasonable access to all relevant information, premises, data, employees, agents, subcontractors and assets at all locations at which the same are present (or may reasonably be expected to be present), including locations from which obligations of the Supplier are being or have been or should have been carried out (but not to information which the Supplier is obliged to keep confidential unless such information is required to verify the items provided under paragraph 1.9.2 and not to information which is legally privileged and/or subject to litigation privilege); and

(b) all reasonable assistance in carrying out any audit.

1.9.4 For the purpose of complying with this paragraph 1.9, the Supplier shall promptly and efficiently give BAT and Audit Right Holders (including i authorised employees of any member of the BAT Group), its any assistance they reasonably require and follow their instructions with regard to such assistance. The Supplier shall also ensure that it maintains the reports in paragraph 1.9.2 in a manner that enables them to be viewed without disclosing any information which may be redacted under 1.9.2.

1.9.5 Any inspection or audit, or failure to inspect or audit, shall not in any way relieve the Supplier from its obligations under this Agreement.

1.9.6 The Supplier shall procure that all relevant Supplier Personnel participate in any audit conducted pursuant to this paragraph 1.9.

1.9.7 For the purposes of this paragraph 1.9, an unlimited number of audits may be conducted in any 12-month period where the relevant audit or audits are required by a Regulatory Authority, conducted for the purposes of investigating suspected fraud or conducted for the purposes of investigating an actual or suspected breach, Security Event or Security Incident.

## SECTION 2: SECURITY INCIDENTS NOTIFICATION AND RESPONSE

### 2.1 Detecting the Occurrence of a Security Event.

**2.1.1** The Supplier shall ensure:

(a) it develops, implements and maintains appropriate technical and organisational measures to identify the occurrence of a Security Event;
(b) discovers Security Events in a timely fashion;
(c) anomalous activity is detected, and the potential impact of Security Events is understood. This will include, but is not limited to ensuring that:
  (i) a baseline of network operations and expected data flows for users and Systems is established, managed and tested;
  (ii) detected events are analysed to understand attack targets and methods;
  (iii) Security Event data is collected and correlated from multiple sources and sensors; and
  (iv) incident alert thresholds are established in line with Best Industry Practice;

(d) Systems are monitored to identify Security Events and verify the effectiveness of protective measures. This will include, but is not limited to ensuring that:

  (i) networks are monitored for potential Security Events;

  (ii) the physical environment is monitored for potential Security Events;

  (iii) personnel activity is monitored for potential Security Events;

  (iv) it monitors Systems for malicious code;

  (v) it monitors Systems for unauthorised mobile code;

  (vi) external service provider activity is monitored to detect potential Security Events;

  (vii) it monitors for unauthorised personnel, connections, devices, and software is performed; and

  (viii) vulnerability scans are performed;

(e) detection processes and procedures are maintained and tested to ensure awareness of anomalous events. This will include, but is not limited to ensuring that:

  (i) detection processes comply with all applicable requirements and are in line with Best Industry Practice;
  (ii) roles and responsibilities for detection are well-defined to ensure accountability;
  (iii) Anomalies and Events wherein are detected in a timely manner and the potential impact of events is understood;

(iv) Security continuous monitoring wherein the Supplier's System and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of the Supplier's protective measures;
(v) detection processes are tested regularly, and in any event no less than once a year;
(vi) Event detection information is communicated to relevant parties to ensure that events are acted upon as required; and
(vii) detection processes are continuously updated in line with Best Industry Practice.

**Responding to Security Incidents.**

**2.2.1** The Supplier shall ensure:

(a) it develops, implements and maintains appropriate technical and organisational measures to respond to a Security Incident, including but not limited to, the ability to reduce the impact of Security Incidents on the rights and freedoms of data subjects;
(b) it contains the impact of a potential Security Incident;
(c) response processes and procedures are executed and maintained, to ensure an effective and timely response to detected Security Incidents;
(d) response activities are coordinated with internal and external stakeholders, and where necessary law enforcement agencies. This will include, but is not limited to ensuring that:

(i) Personnel know their roles and order of operations when a response is needed; and

(ii) Security Incidents are reported consistent with established criteria;

(e) analysis is conducted to ensure its response to a Security Incident is effective and supports recovery of Systems and BAT Data and mitigates potential harm to the rights and freedoms of data subjects. This will include, but is not limited to ensuring that:

(i) Notifications from detection systems are investigated;

(ii) The impact of Security Incidents is understood;

(iii) Forensics are performed where necessary;

(iv) Incidents are categorised consistent with response plans and reporting/notification requirements; and

(v) Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers);

(f) activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
(g) response activities are improved by incorporating lessons learned from current and previous detection/response activities following a detailed and documented post-mortem review.

**2.3 Recovering from Security Incidents.**

2.3.1 The Supplier shall ensure:

(a) it develops, implements and maintains appropriate technical and organisational measures to maintain Resilience and to restore any capabilities or services that were impaired due to a Security Incident;
(b) it develops and implements a plan to reduce the impact of a Security Incident and make a timely recovery to normal operations;
(c) recovery processes and procedures are executed and maintained to ensure restoration of Systems and BAT Data affected by Security Incidents;
(d) recovery planning and processes are improved by incorporating lessons learned into future activities.
(e) restoration activities are coordinated with internal and external parties (e.g. coordinating centres, internet service providers, owners of attacking systems, victims, other CSIRTs, and vendors).

2.3.2 Disaster Recovery and Supplier Contingency Planning.

(a) The Supplier shall ensure that it has in place at all times a business continuity plan, prepared and maintained in accordance with Best Industry Practice, detailing the steps, actions and procedures to be implemented to ensure that the BAT Group continues to receive the Services in accordance with this Agreement, and any adverse effect on the BAT Group is minimised, if any situation occurs for whatever reason that materially adversely impacts on the Supplier's ability to supply the Services or is

likely to do so (a Supply Threat). Business impact assessments, being the initial stage of the business continuity plans, must also include assessments of cyber security threats, like ransomware, malware, cyber-attack, data theft.

(b) The Supplier shall immediately implement the business continuity plan required to be put in place under this paragraph 2.3.2 if a Supply Threat occurs.

(c) The Supplier shall provide a copy of each business continuity plan required to be put in place pursuant to this paragraph 2.3.2 to BAT on request and shall in any event notify BAT of any changes made to it. Where requested by BAT, the Supplier shall arrange discussions between representatives of BAT and appropriate representatives of the Supplier to explain and provide assurances as to the business continuity plans the Supplier has in place and will be maintaining and shall provide BAT with such information as it may reasonably require to satisfy itself that the Supplier is compliant with its obligations in this paragraph. All activities of the Supplier in connection with this paragraph 2.3.2 shall be undertaken at no cost to BAT.

**2.4 Incident Notification and Communication**

2.4.1 The Supplier shall notify BAT immediately or within than 72 (seventy two) hours, if it becomes aware of any actual, threatened or potential Security Event or Security Incident and shall ensure all such notices include full and complete details, to the best of Supplier's knowledge, relating to each and every such actual, threatened or potential Security Event or Security Incident of which the Supplier becomes aware (each such actual, threatened or potential Security Event or Security Incident being hereinafter referred to as a **Security Breach**) where it may impact any BAT Data and in particular:

(a) the nature and type of each Security Breach , the time of its occurrence, its criticality, type, confidentiality and volume of data affected, status of remediation and any other information that may be useful for BAT in order to assess the impact of the Security Breach ;

(b) the nature and facts of each Security Breach including the categories and number of BAT Data records and, if applicable, BAT individuals concerned, categories and approximate numbers of the BAT Data Subjects (and identities of BAT Data Subjects if known);

(c) the contact details of the data protection officer or other representative duly appointed by the Supplier from whom BAT can obtain further information relating to each Security Breach;

(d) the likely consequences or potential consequences of each Security Breach and details of whether any of the BAT Personal Data was encrypted; and

(e) the measures taken or proposed to be taken by the Supplier and/or any Supplier Personnel to address each Security Breach and to mitigate any possible adverse effects and the implementation dates for such measures,

and where, but only in so far as, it is not possible to provide the information referred to in this sub-paragraph 2.4.1 at the same time as the notification, such information shall be provided in phases as soon as that information becomes available (and in such a manner as to enable BAT, or the relevant BAT Affiliate, to meet its notification and documentation obligations).

2.4.2 The Supplier shall co-operate with BAT and all other BAT Affiliates (as required) and take such reasonable commercial steps as are directed by BAT to assist in BAT's (or the relevant BAT Affiliate's) investigation, mitigation and remediation of each Security Breach, and (unless otherwise agreed with BAT) take immediate and appropriate action to stop the Security Breach, recover any BAT Data or other information and fix any vulnerabilities to prevent further breaches.

2.4.3 In the event of a Security Breach, the Supplier shall not inform any third party without first obtaining BAT's prior written consent, unless notification is required under local laws (such as, for example, European Union law) to which the Supplier is subject, in which case the Supplier shall inform BAT of that legal requirement (unless that law prohibits such notification on important grounds of public interest), provide a copy of the proposed notification and consider any comments made by BAT before notifying the breach.

2.4.4 The Supplier shall notify BAT any actual, threatened or potential Security Events and Security Incidents in accordance with the below procedure:

(a) Call duty number: **+48725770054;**

(b) Send an Email: ITSIRT@bat.com marked according to incident priority with CAPITALISED AND CLEAR SUBJECT LINE; and

(c) e mails at a minimum must include the below:

(i) the first email detailing:

- The time period of the Security Breach;
- A description of the data involved;
- Consequences of the Security Breach;
- How the Security Breach was discovered;
- What is needed and when; and

(iii) a follow up e-mail, detailing:

- How the Security Breach was resolved;
- If and how the notification(s) were provided and when.

2.4.5 As a means of secure data exchange:

(i) subject to paragraph 2.4.5 (ii), where sensitive data or large amounts of data is being provided by the Supplier to BAT e.g., for further forensic analysis, BAT will provide access to a dedicated SharePoint/OneDrive space and the Supplier must use such dedicated SharePoint/OneDrive space for the provision of all such data being provided by the Supplier;

(ii) where data designated by BAT as most confidential information (**MCI**) is being provided by the Supplier to BAT, Intralinks VIA workspace access may also be provided by BAT in which case the Supplier must use the Intralinks VIA workspace access for the provision of all MCI being provided by the Supplier.

## SECTION 3: INFRASTRUCTURE OR CLOUD-BASED SERVICES REQUIREMENTS

### 3 Infrastructure or cloud-based services requirements

3.1 In this section 3 the following terms shall have the meanings set out below and cognate terms shall be construed accordingly: the below

**"Cloud Infrastructure Type Services"** means the Supplier is providing the Services on /from/including Cloud infrastructure not managed by BAT. For example, the Supplier in its provision of the Services the Supplier deliver a service where the service is hosted on infrastructure using cloud service providers resources e.g., Amazon Web Services, Google Cloud Platform, Microsoft Azure or other third-party cloud infrastructure provider. In terms of infrastructure, the Supplier is solely responsible for infrastructure operations; and

**"Non-Cloud Infrastructure Type Services"** means the Supplier is providing the Services on/from/including non-Cloud infrastructure not managed by BAT. For example, the Supplier in its provision of the Services is hosting it on its own data centre (or collocation data centre) owned or managed by or for the Supplier where the Supplier and/or any Contractor manages and controls the network, storage, and servers without using the resources of a cloud service provider e.g. Amazon Web Services, Google Cloud Platform, Microsoft Azure or other third party cloud infrastructure provider to host the service .The hardware including its maintenance, the power supply, the provision of the data centre facility as well as virtualization are part of the Supplier's responsibility.

3.2 The Supplier shall adhere to the additional requirements in this section 3 based on the type of Services being provided and its responsibility for the management of the infrastructure or cloud subscriptions:

3.2.1 for **Non-Cloud Infrastructure Type Services** paragraphs 3.3 and 3.4 shall apply; and

3.2.2 for **Cloud Infrastructure Type Services** paragraphs 3.3 and 3.5 shall apply.

### 3.3 Protecting Systems and BAT Data.

3.3.1 The Supplier shall ensure:

(a) access to the Supplier's physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistently with the assessed risk of unauthorised access to authorised activities and transactions. This will include, but is not limited to ensuring that:
  (i) physical access to assets is managed and protected;
  (ii) identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes;
  (iii) remote access to Supplier environment processing any BAT Data is managed through multi-factor authentication;
  (iv) access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties;
  (v) passwords are not transmitted in clear text, displayed on screen or written down either digitally (without encryption), or on paper;
  (vi) identities are proofed and bound to credentials and asserted in interactions; and Users, devices, and other assets processing any BAT Data are authenticated commensurate to Risks to Security (e.g. multi-factor authentication);
  (vii) network integrity is protected (e.g., network segregation, network segmentation);
  (viii) technical security solutions are managed to ensure the Security and Resilience of the Supplier's Systems and BAT Data;

(b) technical security solutions are managed to ensure the Security and Resilience of the Supplier's Systems and BAT Data. This will include, but is not limited to ensuring that:

  (i) backups of information are conducted, maintained, and tested;

  (ii) audit/log records are determined, documented, implemented, and reviewed in accordance with Best Industry Practice;

  (iii) ensuring technical vulnerability management processes are complied with in order to keep software up to date by applying security patches when they are made available. This process will include (1) a policy on vulnerability management including target deployment times for patches of differing criticality ratings; (2) awareness of patch releases; (3) documented awareness of patches missing from the environment; (4) an automatic or manual mechanism to deploy patches across the environment; and (5) a requirement that the most critical patches be applied immediately;

  (iv) the principle of least functionality is incorporated by configuring the Supplier's Systems to provide only essential capabilities;

  (v) communications and control networks are protected;

  (vi) mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations;

  (vii) perimeter defences such as firewalls, intrusion prevention / detection systems and data loss prevention solutions are implemented and maintained;

  (viii) anti-virus or anti-malware systems are implemented and maintained for all Systems;

  (ix) all the Supplier's Systems have secure configuration;

  (x) where the Supplier's Systems are exposed to public networks such as the Internet, they are adequately protected from a range of threats relevant to that possible exposure. This shall include appropriate logical or physical segregation of the Supplier's Systems, authentication requirements, and clearly defined ports and protocols which must be exposed to support the services supplied to BAT including vulnerability scans and penetration testing by a specialist third party. Such penetration test must be repeated annually throughout the duration of any processing of any BAT Data;

3.3.2 Without prejudice to the other provisions of this Schedule, the Supplier shall not implement any material changes in Supplier processes, policies, architecture which adversely impacts or could adversely impact security of BAT Assets or any BAT Data, or the continuity of services to or for any member of the BAT Group or the continuity of the business or operations of BAT, or which increases or could increase the Risks posed to Security, without BAT's prior approval. BAT's approval will not relieve the Supplier of its obligations or liability under the Agreement.

**3.4** The Supplier shall ensure that BAT Data, personnel and all Systems that enable the delivery of the Services are identified and managed consistently with their relative importance to the Security of Systems and BAT Data. This should include ,but is not limited to ensuring that physical devices and the Supplier Systems within the organisation are inventoried.

### 3.5 Miscellaneous

3.5.1 In the event that the Supplier in its provision of Services is providing BAT a SaaS, PaaS, IaaS (including development thereof), the Supplier shall ensure:

(a) all server/hard disks and/or databases handling and / or processing any BAT Data are encrypted according to current Best Industry Practice;

(b) it participates in surveys, questionnaires in order to provide the evidence needed for BAT's IT security compliance assessment;

(c) it provides executive summary reports of periodical vulnerabilities scans and pen tests on assets impacting the any of the Services being provided to BAT and security of BAT Data and/or BAT assets accessible by the Supplier, as applicable for the scope of service provided to BAT. Where applicable, supplier shall facilitate and support web application and other assets vulnerabilities scans and pen tests carried out by BAT of assets dedicated to BAT or owned by BAT, managed by the Supplier;

(d) it remediates any vulnerabilities identified on Supplier assets providing services / data processing for BAT according to criticality and agreed time frames for issue remediations.

## SECTION 4: SECURITY REQUIREMENTS FOR SAAS

### 4. Security requirements for SaaS

4.1 In the event that the Supplier in its provision of Services is providing BAT a SaaS the following additional obligations apply:

(a) Without prejudice to the other provisions of this Schedule, the Supplier shall not implement any material changes to the Supplier's Systems, processes, policies, or architecture which adversely impacts or could adversely impact security of BAT Assets or any BAT Data , or the continuity of services to or for any member of the BAT Group or the continuity of the business or operations of BAT, or which increases or could increase the Risks posed to Security, without BAT's prior approval. BAT's approval will not relieve the Supplier of its obligations or liability under the Agreement.

(b) In a multi-tenant SAAS environment, the Supplier shall ensure that all software application databases and BAT Data are isolated from other tenants and data processed on behalf of any person other than a BAT Group Company and are not readable by SaaS provider employees, staff or contractors, except during Standard Environment Maintenance Activities and to extent approved in advance by BAT in writing. For this purpose, "Standard Environment Maintenance Activities" means standard operations of operators and administrators of the SAAS environment, not including troubleshooting, emergency or other actions requested by BAT and requiring access to any BAT Data.

## 5 Security Requirements for Software Development

5.1 In the event that the Supplier in its provision of Services is providing software development services the following additional obligations apply:

5.1.1 The Supplier shall provide development and maintenance teams with relevant processes, procedures and tools, to enable introduction of secure code/systems whether that is a new development, or a maintenance change, that the code/system meets secure coding standards, and secure configuration standards. This includes, but is not limited to: carrying out periodic secure coding trainings for developers, and implementing DevSecOps process and toolkit, including security testing, in accordance with BAT requirements as set out in BAT's DevSecOps Playbook, as updated and provided to the Supplier from time to time and any other supporting documentation of process metric and controls provided by BAT from time to time.

5.1.2 Without prejudice to the other provisions of this Schedule, the Supplier shall not implement any material changes in Supplier processes, policies, architecture which adversely impacts or could adversely impact security of BAT Assets or any BAT Data, or the continuity of services to or for any member of the BAT Group or the continuity of the business or operations of BAT, or which increases or could increase the Risks posed to Security, without BAT's prior approval. BAT's approval will not relieve the Supplier of its obligations or liability under the Agreement.

5.1.3 Prior to the implementation of any changes to BAT production systems, the Supplier shall, as applicable, perform relevant set of controls to ensure it detects software vulnerabilities:

(a) Carry out code and configuration review / static application security testing (SAST);
(b) Data reviews;
(c) Dynamic application security testing (DAST) and penetration testing;
(d) Where any code contains third party components or open source libraries, the Supplier properly document the relevant third party components and open source libraries (in form of inventory), obtain BAT prior approval of using Open Source prior to implementation of the code, and ensure that relevant threats, including 'backdoors' and vulnerabilities hidden in the used code and/or libraries are clearly identified and fully addressed by implementing relevant controls and tools, e.g. software composition analysis (SCA) tools and any other means consistent with Best Industry Practice; and
(e) The Supplier shall conduct all reviews in connection with this Schedule in relation to source code and system security in accordance with the Segregation of Duties (SOD) principle.

5.1.4 The Supplier shall employ an adequate level of automation in relation to all development activities, including but not limited to, with respect to the following:

(a) testing activities integrated into DevSecOps and CI/CD workflows; and
(b) monitoring of security vulnerabilities with prioritization and reporting of findings and recommendations.

5.1.5 The Supplier shall ensure that the results of all security tests are properly documented. All issues are remediated prior to their promotion to a production environment. The Supplier shall perform security tests to evidence secure code prior to promotion to the production environment.

5.1.6 The Supplier shall measure secure development related performance indicators, e.g., cost of security remediation, time to patch, ratio of failing security tests and number of vulnerabilities found, in accordance with such metrics consistent with Best Industry Practice as BAT may reasonably require, and shall provide BAT with a report in relation thereto with the objective of measuring and reporting on the effectiveness of the security elements of all development processes

5.1.7 In relation to all development activities:

(a) the Supplier shall only use in production versions of code approved in advance by BAT in writing;
(b) where applicable, the Supplier shall adhere to infrastructure as code and security as code principles to ensure security by design and consistency between various solution components and features;
(c) the final version of any Source Code delivered under this Agreement shall be delivered to a repository designated by BAT.