



Information Security

Term	Definition
Affiliate:	means an entity that, either directly or indirectly, controls, is controlled by, or is under common control with, the relevant entity, where “control” means the ability to direct the affairs of another by ownership, contract or otherwise.
Agreement:	means the agreement between the Client and the Supplier for the provision of the Services which incorporates this information security schedule.
Asset:	means: (i) any item or element of hardware, software or equipment that is or may be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting data of any type (including voice); and (ii) any documentation (in whatever medium) that relates to the use or operation of such items and elements.
Client:	means the person purchasing the Services under the Agreement.
Client Data:	means: (a) any Personal Data in respect of which any member of the Client Group is a data controller; (b) any data that any member of the Client Group controls, provides or has in its possession; and (c) any data that the Supplier (either itself or through others) gathers, creates or processes for the Client.
Client Group:	means the Client and all its Affiliates (and “member of the Client Group” shall be construed accordingly).
Client Information Systems:	means information technology and communications systems, networks, services and solutions (including all Assets that either (a) form part of such systems and networks, or (b) are used in the provision of such services and solutions) which are owned by or reserved for operation by or on behalf of any member of the Client Group.
Data Subject:	means an identified or identifiable natural or legal person; an “identifiable” person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Good Security Practice:	means measures and practices consistent with: (a) the technical and organisational measures and practices that are required by, or recommended in, internationally accepted management standards and codes of practice relating to Information Security (such as ISO/IEC 27001 (Information Security Management Systems – Requirements) and ISO/IEC 27002 (Code of Practice for Information Security Management)); and (b) security standards and guidelines (including generally accepted principles regarding the segregation of the duties of governance, implementation, administration and control) and techniques such as strong authentication, access control and auditing, “least privilege” assignment, all as reasonably made available to the general public or information security practitioners and stakeholders by generally recognised authorities and organisations regarding Information Security, as the same are expanded, varied and replaced from time to time.
Information Security:	means: (a) the protection and assurance of: (i) the confidentiality, integrity, reliability and availability of information and information systems; and (ii) related properties of information such as authenticity, accountability, and non-repudiation; and (b) compliance with all regulations applicable to the Processing of information.
Personal Data:	means any information relating to a Data Subject.
references to “personnel”:	such references include also references to the relevant party’s subcontractors and service providers.
to “Process” (and variants of it, such as “Processing”):	means to perform any operation or set of operations upon data, whether or not by automatic means, such as collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making available), aligning or combining, blocking, erasing or destroying.



PHILIP MORRIS INTERNATIONAL

Services:	means the services being provided by the Supplier under the Agreement.
Supplier:	means the person providing the Services to the Client under the Agreement.

The Supplier shall:

- (a) provide the Services and perform its obligations under the Agreement in accordance with:
 - (i) this information security schedule; and
 - (ii) Good Security Practice; and
- (b) implement the technical and organisational measures described in the table below (the “**Security Measures**”), in particular in respect of:
 - (i) its: (A) technical infrastructure; (B) application infrastructure; and (C) telecommunications infrastructure;
 - (ii) the operation, monitoring and security of its infrastructure systems; and
 - (iii) any software it makes available as part of the Services.

Type of Security Measures	Details of the Security Measures
Compliance with internal policies:	<ol style="list-style-type: none"> 1. The Supplier has issued, and shall implement and maintain, internal policies that: <ol style="list-style-type: none"> (a) require employees to keep Client Data confidential and to comply with the Supplier’s technical and organisational measures established to protect confidential Client Data; and (b) govern, at a minimum: <ol style="list-style-type: none"> (i) use of computers, portable devices, e-mail, and internet; and (ii) how to protect company information and Personal Data. 2. The Supplier shall: <ol style="list-style-type: none"> (a) train its employees and relevant third parties (such as contractors) on these policies and on related IS and security aspects; and (b) require its employees, and relevant third parties, to follow these policies. Employees and contractors are specifically instructed not to share or write down passwords.
Building access controls:	<p>The Supplier controls access to its buildings, including with:</p> <ol style="list-style-type: none"> 1. access cards, video monitoring or other checks (or any combination of the foregoing); and 2. automatic mechanisms to monitor the environment and trigger alarms in case of intrusion attempts. <p>To the extent that the Supplier Processes Client Data otherwise than directly on Client Information Systems, the Supplier shall also have automatic mechanisms to monitor the environment and trigger alarms in case of inappropriate conditions for operating computer systems due to (amongst others) fire, temperature, electrical power, or humidity.</p>
System access controls:	<p>The Supplier shall:</p> <ol style="list-style-type: none"> 1. restrict access to systems that contain Client Data; 2. Process Client Data only (a) through devices (including servers, workstations (such as desktop computers and laptop computers), and handheld mobile devices (e.g. PDAs, smartphones etc.)) effectively controlled by the Supplier; or (b) within Supplier controlled applications; and, in both cases, adequately protect the Client Data at rest and in transit; 3. keep a list of the locations of the centres where its personnel Process Client Data under its control; 4. maintain access control lists to production systems and the permissions granted to user accounts; 5. maintain specifications of technical and organisational resources (covering computer system authentication, authorization and accounting) required to ensure the confidentiality, integrity and availability of the data that are Processed; 6. restrict access to the Client’s information systems to those personnel who need access for the purposes of providing the Services, and ensure that such personnel access only such parts of the Client’s information systems as are necessary for the purposes of providing the Services;



Type of Security Measures	Details of the Security Measures
	<p>7. review user access privileges used by or on behalf of the Supplier to access the Client’s information systems with the frequency required by the Supplier’s security policies and in any event no less frequently than once per calendar year; and</p> <p>8. ensure that any personnel who have access to the Client’s information systems act responsibly, with due care.</p> <p>To the extent that the Supplier Processes Client Data otherwise than directly on Client Information Systems, the Supplier shall also ensure that master versions of Client Data are located only on network servers that satisfy all of the following conditions: (i) they are effectively controlled by the Supplier; (ii) they are secure; and (iii) they have restricted system access.</p>
<p>Internal security management procedures:</p>	<p>To the extent that the Supplier Processes Client Data otherwise than directly on Client Information Systems, the Supplier has established, and implements, internal security management procedures that cover the following elements:</p> <ol style="list-style-type: none"> 1. requesting and approving data processing rights in the Supplier’s computer systems; granting such rights in the systems; and who is responsible for requesting, approving, granting and reviewing such rights; 2. methods and resources for authenticating computer system users, and procedures relating to managing and using such methods and resources; 3. how to create and use copies of system data, programs and program tools used for backing-up and restoring computer systems, as well as how to create and maintain system data required for computer system testing and migration; 4. the appropriate protection of any copies required for system backup, archiving and other purposes; 5. how to secure computer systems against unauthorised system access; 6. how computer systems record who has accessed such systems, stating the date and scope of such access; 7. how to conduct reviews and maintenance of media and systems used for data Processing; 8. how to dispose securely of information that no longer needs to be retained; and 9. procedures to detect and prevent security incidents, including: (i) asset management; (ii) impact assessment; and (iii) prompt remediation and escalation to all appropriate parties.
<p>Computer access controls:</p>	<p>The Supplier shall control access to its computers and its security of the underlying infrastructure by:</p> <ol style="list-style-type: none"> 1. automatically disabling user IDs after 5 invalid login attempts; 2. installing and maintaining up-to-date adequate protection against malicious software; 3. maintaining security with regard to the internet through firewalls and other measures that address unauthorised attempts to access applications, sites or services that are available through the internet, or to access data transmitted over the internet; 4. restricting access to system features (including computer system configuration settings) and other tools relevant for computer system security to authorised personnel; and 5. applying cryptographic protection measures to data used for authentication (e.g. hash passwords using industry accepted and generally secure algorithms). <p>The Supplier shall, in addition, perform the following:</p> <ol style="list-style-type: none"> 6. provision and de-provision end user IDs; enable basic authentication and single-sign-on that require a valid individual user ID and password; 7. enforce a password policy that (a) requires that each password comprises 8 or more characters and contains at least three of the following four character groups: (i) lowercase letters (a through z); (ii) uppercase letters (A through Z); (iii) numerals (0 through 9); and (iv) special characters (such as !, \$, #, %); and (b) makes passwords automatically expire within pre-defined intervals; after expiry, a new password must be created; 8. automatically lock idle individual computer logon sessions after a set period of up to 15 minutes; and



Type of Security Measures	Details of the Security Measures
	<p>9. manage user rights, logins and passwords.</p> <p>To the extent that the Supplier permits the Client to itself manage users' access rights to the Supplier's systems, the Supplier shall:</p> <p>10. ensure the Client's access to such systems is secure; and</p> <p>11. provide the Client with such tools that enable it to perform the functions set out in paragraphs 6 to 9 above.</p>
Processing Client Data:	<p>To the extent that the Supplier Processes Client Data otherwise than directly on Client Information Systems, the Supplier shall maintain and enforce procedures relating to the transmission and protection of information and Client Data, including:</p> <ol style="list-style-type: none"> 1. maintaining guidelines for retention and disposal of business correspondence and other records; 2. maintaining policies regulating the downloading, use and retention of third party software and data; 3. ensuring the information security of Client Data that is electronically transmitted (directly or via staging facilities) between separate business systems (whether at the Supplier's or other parties' facilities); 4. managing removable and portable media in accordance with Good Security Practice, including as appropriate: <ol style="list-style-type: none"> (a) storing them in a safe, secure environment in accordance with manufacturers' specifications; (b) ensuring their secure transport, erasure and disposal; and (c) storing back-up media in a remote location, at a sufficient distance to escape any damage from a disaster at the main site; 5. protecting Client Data in transit and at rest using Good Security Practices such as encryption and access controls; 6. restricting access to Client Data to those personnel who need access for the purposes of providing the Services, and ensuring that such personnel Process such Client Data only to the extent necessary for the purposes of providing the Services; and 7. returning all Client Data to the Client where the Supplier no longer requires access to, or use of, such Client Data for the purposes of providing the Services; and 8. once the Client has confirmed to the Supplier in writing that any Client Data returned to it pursuant to paragraph 7 above has been successfully received, deleting all such Client Data.
Managing Assets:	<p>If the Supplier is to decommission, or dispose of, any Asset containing Client Data, the Supplier shall ensure either:</p> <ol style="list-style-type: none"> 1. that the Asset is irretrievably destroyed or returned to the Client; or 2. that the Client Data or relevant information held on the Asset is deleted and rendered irrecoverable prior to decommissioning, or disposing of, the Asset.
Transmissions:	<ol style="list-style-type: none"> 1. The Supplier shall not transmit, or request any user to transmit, passwords in clear text over information systems or between information systems. 2. The Supplier shall not transmit, or permit the transmission by any member of its personnel of, any unstructured data to/from the Client or any of its Affiliates using any means other than through the Supplier's corporate systems. As part of the foregoing, for the purpose of hosting or transmitting unstructured data as part of the Services, or for the purpose of hosting or transmitting Client Data, the Supplier shall not use, and shall not permit, the use of for this purpose of: <ol style="list-style-type: none"> (a) non-corporate e-mail accounts (e.g. Yahoo!, Gmail, etc.); (b) unsecured FTP; or (c) consumer file sharing services. 3. The Supplier shall not send any CD/DVD/disk media containing Client Data to any recipient (including the Client or any of its Affiliates) via any postal or courier service except with the prior written agreement of the Client's designated security contact. Where the Supplier requests and obtains such written agreement, such approval shall be valid for such individual transmission only.



Type of Security Measures	Details of the Security Measures
Review, reports, notification:	<ol style="list-style-type: none"> 1. The Supplier shall take appropriate measures to review that: <ol style="list-style-type: none"> (a) it complies with this Schedule; and (b) the measures it takes in compliance with this Schedule are effective to achieve Good Security Practice. 2. To the extent that the Supplier uses a web-based solution to either Process Client Data or provide the Services: <ol style="list-style-type: none"> (a) the Supplier shall perform web application security assessments annually and discuss the results with the Client upon request; and (b) the Client may perform its own web application security assessment of the Supplier's systems non-production environments after coordinating with the Supplier to agree on the timing and scope of the assessment. 3. The Supplier shall provide the Client, no less frequently than each month (or such other period as the Client may agree), with comprehensive and readily understandable overviews regarding: <ol style="list-style-type: none"> (a) the access permissions of all persons with access to the Client Data; and (b) audit trails of all persons with access to the Client Data. 4. The Supplier shall, within a reasonable period, notify the Client if the Supplier experiences a security event that negatively affects the confidentiality or integrity of Client Data.
Service continuity:	<p>The Supplier shall:</p> <ol style="list-style-type: none"> 1. detect, track, escalate and resolve any actual (or potential) incidents, failures, security events or other operational risks in a timely manner; 2. test, approve and deploy changes to the Supplier's information systems in a controlled manner with only minimal disruption to the Client; 3. plan, implement and regularly test the appropriate organisational and technical measures necessary to sustain or rapidly recover the services being provided to the Client in the case of any reasonably foreseeable disruptive event; and 4. ensure that any stand-by or alternative location used for the purposes of the Supplier's service continuity is subject to information security controls at least equivalent to those in force at the facility from which the Supplier usually operates the relocated processes.