ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Введение

Настоящее Приложение устанавливает обязательства в отношении информационной безопасности, которым должен соответствовать Поставщик при оказании услуг Филип Моррис Казахстан (ФМК).

2. Определения

a) **Данные ФМК** означают
- i) любые Персональные Данные, переданные ФМК Исполнителю;
- ii) любые данные, которыми управляет, которые предоставляет или имеет во владении ФМК; и
- iii) любые данные, которые Поставщик (сам или через посредников) собирает, создает или обрабатывает для ФМК.

b) **Ресурс** означает (i) любой компонент или элемент аппаратных средств, программного обеспечения или оборудования, который используется или может использоваться с целью создания, доступа, обработки, защиты, наблюдения, хранения, извлечения, отображения или передачи данных любого типа (включая голосовые); а также (ii) любую документацию (на любом носителе), которая относится к использованию или управлению такими предметами или элементами.

c) **Передовые практические методы в области безопасности** означают меры и практические методы, согласующиеся с техническими и организационными мерами и практическими методами, установленными в качестве необходимых или желательных

INFORMATION SECURITY

1. Introduction

This Schedule sets out the obligations regarding Information Security with which the Supplier is required to comply in providing services to Philip Morris Kazakhstan (PMK).

2. Definition

a) **PMK data** mean
- i) any Personal Data transferred by PMK to the Supplier;
- ii) any data that PMK controls, provides or has in its possession; and
- iii) any data that the Supplier (either itself or through others) gathers, creates or processes for PMK.

b) **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.

c) **Best security practices** mean measures and practices consistent with the technical and organizational 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

общепринятыми международными стандартами управления и практическими руководствами в области Международной безопасности (например, ISO/IEC 27001 (СУИБ – Требования) и ISO/IEC 27002 (Практическое руководство в области управления информационной безопасностью).

(Information Security Management Systems – Requirements) and ISO/IEC 27002 (Code of Practice for Information Security Management).

d) **Информационная безопасность** означает организацию защиты и обеспечение конфиденциальности, защищенности, надежности и доступности информации и информационных систем; а также наличия соответствующих характеристик безопасности, например, аутентификация, возможность контроля и предотвращение отказа.

d) **Information security** means organization and assurance of the confidentiality, integrity, reliability and availability of information and information systems for authorized persons; and availability of appropriate security features, such as authentication, the ability to monitor and prevent failure.

e) **Персональные данные** означают сведения, относящиеся к определенному или определяемому на их основании оъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

e) **Personal data** mean any information, related to the data subject, specific or defined on their basis, recorded on an electronic, paper and (or) other physical media.

f) **Информационная система ФМК** означает информационные технологии и системы коммуникации, сети, службы и решения (включая все Ресурсы, которые либо (i) составляют часть таких систем и сетей; или (ii) используются для предоставления таких услуг и решений), которые принадлежат или зарезервированы для работы ФМК или от его имени.

f) **PMK 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 PMK.

g) **Осуществлять обработку** (и его варианты, такие как, например, "Обработка") означает выполнение действий или ряда действий в отношении данных, при помощи средств автоматизации или без них, например, сбор, запись, организацию, хранение, адаптацию или изменение, извлечение, обращение за справкой,

g) **Process»** (and variants of it, such as «Processing») to perform an operation or set of operations (e.g. upon Personal Data), whether or not by automatic means, such as collecting, recording, registering, organizing, accumulation, storing, change, addition, adapting or altering, retrieving, consulting, using, disclosing (or otherwise making

использование, раскрытие (посредством передачи, распространения или предоставления любым другим способом), выверка или объединение, блокировка, стирание или уничтожение.

available) by transmission, dissemination, depersonalization or otherwise, aligning or combining, blocking or performing dispersed erasure or destruction.

3. Обеспечение информационной безопасности

3.1. Исполнитель обязан:

a) выполнить свои обязательства в соответствии с настоящим Приложением по обеспечению информационной безопасности; а также Передовыми практическими методами в области безопасности; а также

b) защищать Данные ФМК, включая путем внедрения технических и организационных мер, представленных ниже.

3. Ensuring Information Security

3.1.The Supplier shall:

a) provide the Services and perform its obligations in accordance with this Schedule and Best practices in the sphere of security; and

b) protect PMK Data, including by implementing technical and organizational measures, described below.

4. Соответствие нормам внутренних политик Исполнителя

4.1. Исполнитель должен разработать внутренние политики, которые:

a) регулируют пользование компьютерами, переносными устройствами, электронной почтой и интернетом;

b) обязывают персонал, получивший доступ к Данным ФМК для проведения технического обслуживания с согласия ФМК, сохранять конфиденциальность Данных ФМК и действовать в соответствии с техническими и организационными мерами Исполнителя, принятыми для защиты конфиденциальных Данных ФМК;

c) содержат методы защиты Данных ФМК.

4.2. Исполнитель обязан провести обучение персонала в области своих внутренних политик, и обеспечить выполнение положения таких политик.

4. Compliance with internal policies

4.1. The Supplier shall issue internal policies that:

a) govern use of computers, portable devices, e-mail, and internet;

b) require the Supplier’s employees to keep PMK Data confidential and to comply with the Supplier’s technical and organizational measures established to protect confidential PMK Data;

c) contain methods of protecting PMK Data.

4.2. The Supplier shall train its employees on these policies and ensure compliance of these polices.

5. Контроль за доступом в здание

5.1. Исполнитель обеспечивает контроль за доступом в свои здания, в которых Данные ФМК могут обрабатываться с применением следующего:

a) персональные карточки доступа, видеонаблюдение и иные способы проверки (или сочетание таких мер); а также
b) установки механизмов наблюдения доступа (любые попытки доступа) и включения сигнала тревоги в случае несанкционированного проникновения или попытки проникновения.

5.2. Дополнительно Исполнитель должен обеспечить наличие механизмов наблюдения за прилегающей территорией и включения сигнала тревоги в случае возникновения неприемлемых условий функционирования вычислительных систем в результате (помимо прочего) пожара, экстремальных температур, перебоев в подаче электроэнергии или высокой влажности.

6. Контроль за доступом в системы, используемые Исполнителем

6.1. Исполнитель обязуется:

a) ограничить доступ к системам, которые содержат Данные ФМК;
b) обрабатывать Данные ФМК только посредствам устройств (серверов, рабочих станций (такие как настольные компьютеры и ноутбуки) и портативных мобильных устройств (например, КПК, смартфоны и т.д.)), управляемых Поставщиком или обрабатывать Данные ФМК строго посредством приложений, управляемых Поставщиком, и надлежащим образом защищать их при хранении и передаче;

5. Building access controls

5.1. The Supplier controls access to its buildings, where PMK Data are processed, including with:

a) access cards, video monitoring or other checks (or any combination of the foregoing); and
b) automatic mechanisms to monitor the environment and trigger alarms in case of intrusion attempts.

5.2. 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.

6. System access controls

6.1. The Supplier shall:

a) restrict access to systems that contain PMK Data;
b) process PMK Data only through devices (being servers, workstations (such as desktop computers and laptop computers), and handheld mobile devices (e.g. PDAs, smartphones etc.)) effectively controlled by the Supplier or Process PMK Data only within the Supplier controlled applications and adequately protect PMK Data at rest and in transit;
c) keep a list of the locations of the centres where its personnel Process PMK Data under its control;

c) поддерживать список мест, где персонал обрабатывает Данные ФМК под контролем Поставщика;

d) поддерживать в актуальном состоянии списки по контролю за доступом для производственных систем и разрешения, выданные учетным записям пользователей;

e) защищать Данные ФМК, применяя ограничения доступа, аналогичные существующим в производственных средах, при разработке программного обеспечения или проведении тестирования, когда требуется доступ к Данным ФМК или создаются копии Данных ФМК;

f) поддерживать в актуальном состоянии спецификации технических и организационных ресурсов (покрывающих аутентификацию, авторизацию и управление учетными записями в компьютерной системе), необходимых для обеспечения конфиденциальности, целостности и доступности Обрабатываемых данных;

g) ограничить доступ к Информационным системам ФМК персоналу, который нуждается в нем с целью предоставления Услуг, и убедиться, что этот персонал имеет доступ лишь в те части Информационной системы ФМК, к которым ему необходим доступ для целей оказания Услуг;

h) пересматривать права доступа, используемые Поставщиком или от его имени, для доступа к Информационным системам ФМК с частотой, предусмотренной в политике безопасности Поставщика, и в любом случае не реже одного раза в год; и

d) maintain access control lists to production systems and the permissions granted to user accounts;

e) where the Supplier requires access to, or copies of, any PMK Data for the purposes of software development or testing, protect PMK Data with the same system access restrictions as apply for PMK data in production environments;

f) maintain specifications of technical and organizational resources (covering computer system authentication, authorization and accounting) required to ensure the confidentiality, integrity and availability of the data that are Processed;

g) restrict access to the PMK'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 PMK's information systems as are necessary for the purposes of providing the services;

h) review user access privileges used by or on behalf of the Supplier to access the PMK'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

i) ensure that any personnel who have access to PMK's information systems act responsibly, with due care.

i) убедиться, что любой персонал, имеющий доступ к Информационным системам ФМК, действует ответственно и с должным вниманием.

В случае, если Поставщик обрабатывает Данные ФМК вне Информационных систем ФМК, Поставщик должен гарантировать, что исходная версия Данных ФМК расположена только на сетевых серверах, удовлетворяющих следующим условиям: (i) они эффективно контролируются Поставщиком; (ii) они безопасны; и (iii) они имеют ограниченный доступ к системе.

To the extent that the Supplier Processes PMK Data otherwise than directly on PMK Information Systems, the Supplier shall also ensure that master versions of PMK 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.

7. Внутренние процедуры управления безопасностью

Если Исполнитель осуществляет Обработку Данных ФМК не в Информационных системах ФМК, Исполнитель внедрит и будет выполнять внутренние процедуры управления безопасностью, включающие следующие компоненты:

a) запрос и утверждение прав на обработку данных в вычислительных системах Исполнителя; предоставление таких прав в системах; указание ответственных лиц за направление запросов о предоставлении таких прав, утверждение, предоставление и пересмотр таких прав;
b) методы и ресурсы, используемые для идентификации пользователей вычислительной сети, а также процедуры по управлению и использованию таких методов и ресурсов;
c) методы создания и использования копий системных данных, программ и программных средств, используемых для копирования из архива и восстановления вычислительных систем, а также методы создания и администрирования системных

7. Internal security management procedures

To the extent that the Supplier Processes PMK Data otherwise than directly on PMK Information Systems, the Supplier has established, and implements, internal security management procedures that cover the following elements:

a) 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;
b) methods and resources for authenticating computer system users, and procedures relating to managing and using such methods and resources;
c) 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;

данных, необходимых для осуществления тестирования и переноса вычислительных систем;

d) надлежащая защита копий, необходимых для резервирования и архивирования системных файлов или в иных целях;
e) методы обеспечения безопасности вычислительных систем от несанкционированного доступа;
f) методы регистрации Системами лиц, входящих в такие Системы, указание даты и объема такого доступа;
g) методы проведения обзора и обслуживания средств и Систем, используемых для Обработки данных;
h) методы безопасного уничтожения информации, в сохранении которой больше нет необходимости; а также процедуры по обнаружению и предотвращению нарушений безопасности, включая: (i) управление ресурсами; (ii) оценка последствий; а также (iii) незамедлительное исправление и передача всем соответствующим сторонам.

8. Осуществление обработки данных ФМК

В случае Обработки Исполнителем данных ФМК не в Системах ФМК, Исполнитель обеспечит использование и реализацию процедур, регулирующих передачу и защиту информации и данных ФМК, включая:

a) утверждение и исполнение принципов хранения и уничтожения деловой переписки и других записей;
b) утверждение политик, регулирующих скачивание, использование и хранение программного обеспечения и данных третьих лиц;
c) обеспечение информационной безопасности данных ФМК, передаваемых в электронной форме (напрямую или через средства переноса данных) между отдельными информационными системами (через

d) the appropriate protection of any copies required for system backup, archiving and other purposes;
e) how to secure computer systems against unauthorized system access;
f) how computer systems record who has accessed such systems, stating the date and scope of such access;
g) how to conduct reviews and maintenance of media and systems used for data Processing;
h) how to dispose securely of information that no longer needs to be retained; and procedures to detect and prevent security incidents, including: (i) asset management; (ii) impact assessment; and (iii) prompt remediation and immediate information of all appropriate parties.

8. Processing PMK Data

To the extent that the Supplier Processes PMK Data otherwise than directly on PMK Information Systems, the Supplier shall maintain and enforce procedures relating to the transmission and protection of information and PMK Data, including:

a) maintaining guidelines for retention and disposal of business correspondence and other records;
b) maintaining policies regulating the downloading, use and retention of third party software and data;
c) ensuring the information security of PMK Data that is electronically transmitted (directly or via staging facilities) between separate business systems (whether at the Supplier's or other parties' facilities);

средства переноса данных Исполнителя или иных лиц);

d) управление съемными или переносными носителями в соответствии с Передовыми практическими методами в области безопасности, включая, при необходимости:

e) хранение их в безопасной, защищенной среде в соответствии с техническими требованиями производителя;

f) обеспечение их безопасной транспортировки, стирание и уничтожение; а также

g) хранение резервных носителей в удаленном местонахождении, на достаточном расстоянии во избежание их повреждения в случае аварии на основном объекте;

h) защиту данных ФМК в местах хранения и в пути с использованием таких Передовых практических методов в области безопасности, как, например, шифрование и контроль за доступом;

i) предоставление доступа к данным ФМК только тем сотрудникам, которым такой доступ необходим в целях предоставления Услуг, и обеспечить доступ таких сотрудников к Обработке данных ФМК только в объеме, необходимом для предоставления Услуг;

j) возврат ФМК всех данных ФМК, в случае если Исполнителю в целях предоставления Услуг больше не требуется доступ или использование таких данных ФМК; а также

k) уничтожение всех данных ФМК после получения Исполнителем от ФМК письменного подтверждения об успешном получении ФМК данных ФМК в соответствии с п.j выше.

d) managing removable and portable media in accordance with Best Security Practice, including as appropriate:

e) storing it in a safe, secure environment in accordance with manufacturers' specifications;

f) ensuring its secure transport, erasure and disposal; and

g) storing back-up media in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

h) protecting PMK Data in transit and at rest using Best Security Practices such as encryption and access controls;

i) restricting access to PMK Data to those personnel who need access for the purposes of providing the Services, and ensuring that such personnel Process such PMK Data only to the extent necessary for the purposes of providing the Services; and

j) returning all PMK Data to the PMK where the Supplier no longer requires access to, or use of, such PMK Data for the purposes of providing the Services; and

k) once the PMK has confirmed to the Supplier in writing that any PMK Data returned to it pursuant to paragraph j above has been successfully received, deleting all such PMK Data.

9. Управление Ресурсами

9. Managing Assets

Если Исполнителю необходимо будет списать или уничтожить какие-либо Активы, содержащие данные ФМК по требованию ФМК, Исполнитель обеспечит нижеследующее:

a) безвозвратное уничтожение Актива (только после передачи данных ФМК) или его возврат ФМК; или
b) уничтожение данных ФМК или соответствующей информации, имеющейся на Активе, или обеспечение невозможности их восстановления до списания или уничтожения Актива с согласия ФМК.

If the Supplier is to decommission, or dispose of, any Asset containing PMK Data, the Supplier shall ensure either:

a) that the Asset is irretrievably destroyed or returned to the PMK, or

b) that the PMK Data or relevant information held on the Asset is deleted and rendered irrecoverable prior to decommissioning, or disposing of, the Asset.

10. Передачи

10.1. Поставщик не должен передавать или просить каких-либо пользователей передавать пароли в открытом виде через информационные системы или между информационными системам;

10.2. Поставщик не должен передавать или разрешать передачу своему персоналу любых неструктурированных данных к/от ФМК, с использованием каких-либо средств, кроме как корпоративные системы Поставщика. В рамках вышесказанного, в целях непосредственного хранения или передачи неструктурированных данных, как части услуг, или для цели хранения или передачи Данных ФМК, Поставщик не должен использовать и не должен разрешать использование для этих целей следующего:

a) некорпоративную электронную почту (например, Yahoo!, Gmail и др.);
b) небезопасные FTP;
c) сервисы обмена файлами.

10.3. Поставщик не должен отправлять какие-либо медиа/CD/DVD, содержащие данные ФМК, любым адресатам (включая ФМК) с привлечением любой почтовой или курьерской службы, за исключением случаев предварительного

10. Transmissions

10.1. The Supplier shall not transmit, or request any user to transmit, passwords in clear text over information systems or between information systems.

10.2. The Supplier shall not transmit, or permit the transmission by any member of its personnel of, any unstructured data to/from the PMK 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 PMK Data, the Supplier shall not use, and shall not permit, the use of for this purpose of:

a) non-corporate e-mail accounts (e.g. Yahoo!, Gmail, etc.);
b) unsecured FTP; or
c) consumer file sharing services.

10.3. The Supplier shall not send any CD/DVD/disk media containing PMK Data to any recipient via any postal or courier service except with the prior written agreement of the PMK's designated contact. Where the Supplier requests and obtains such written agreement, such

согласования в письменном виде с контактным лицом ФМК. Если поставщик запрашивает и получает такое письменное согласие, то это одобрение должно быть действительно только для конкретной передачи.

approval shall be valid for such individual transmission only.

11. Обзоры, отчеты, уведомления

11.1. Исполнитель предпримет все необходимые меры для ознакомления с нижеизложенным:

a) ходом соблюдения требований настоящего приложения по обеспечению информационной безопасности; а также
b) действиями, предпринимаемыми им в соответствии с настоящим приложением, которые являются эффективными при реализации Передовых практических методов в области безопасности.

11.2. В случае если Поставщик использует для обработки Данных ФМК или для оказания услуг решения, основанные на Web или мобильном решении, в таких случаях:

a) Поставщик обязан ежегодно проводить оценку безопасности веб-приложения или мобильного приложения и по запросу обсудить результаты с ФМК; и
(b) ФМК может проводить собственную оценку безопасности веб-приложения или мобильного приложения, после взаимного согласования с Поставщиком сроков и границ этой оценки;

11.3. Не реже раза в месяц квартал (или другой такой же период, согласованный с ФМК) Поставщик должен предоставлять ФМК удобные и доступные для понимания отчеты относительно:

a) прав доступа всех работников, имеющих доступ к Данным ФМК;

11. Review, reports, notification

11.1. The Supplier shall take appropriate measures to review that:

a) the Supplier complies with this Schedule; and
b) the measures it takes in compliance with this Schedule are effective to achieve Best Security Practice;

11.2. To the extent that the Supplier uses a web-based or mobile solution to either Process PMK Data or provide the services:

a) the Supplier shall perform web application security assessments of such web-based or mobile solution annually and discuss the results with the PMK upon request; and
b) the PMK may perform its own web application security assessment of such web-based or mobile solution of the Supplier's systems non-production environments after coordinating with the Supplier to mutually agree on the timing and scope of the assessment.

11.3. The Supplier shall provide PMK, no less frequently than each quarter (or such other period as PMK may agree), with comprehensive and readily understandable overviews regarding:

a) the access permissions of all persons with access to the PMK Data; and

b) журналы контроля работников с доступом к Данным ФМК.

11.4. Поставщик обязан в разумный срок уведомить ФМК о произошедшем событии, связанного с безопасностью, негативно сказывающимся на конфиденциальности или целостности Данных ФМК.

b) audit trails of all persons with access to the PMK Data.

11.4. The Supplier shall, within a reasonable period, notify the PMK if the Supplier experiences a security event that negatively affects the confidentiality or integrity of PMK Data.

12. Бесперебойность предоставления услуг

12.1. Исполнитель:

a) своевременно выявит, отследит, и разрешит фактические (или потенциально возможные) ситуации, неисправности, события в системе безопасности и другие операционные риски;

b) под необходимым контролем проведет тестирование, утвердит и внесет изменения в информационные системы Исполнителя лишь с минимальным прерыванием деятельности ФМК;

c) осуществит планирование, внедрение и регулярную проверку соответствующих организационных и технических мер, необходимых для продолжения или быстрого восстановления предоставления ФМК услуг в случае наступления внештатной ситуации, которую можно обоснованно предвидеть; а также

d) обеспечит, чтобы использование запасных или альтернативных объектов в целях продолжения оказания услуг Исполнителем осуществлялось с учетом мер по контролю секретности информации, которые как минимум эквиваленты мерам, действующим на объекте, на котором Исполнитель обычно

12. Service continuity

The Supplier shall:

a) detect, track, escalate and resolve any actual (or potential) incidents, failures, security events or other operational risks;

b) test, approve and deploy changes to the Supplier's information systems in a controlled manner with only minimal inconvenience to the PMK;

c) plan, implement and regularly test the appropriate organisational and technical measures necessary to sustain or rapidly recover the services being provided to the PMK in the case of any reasonably foreseeable disruptive event; and

d) 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.

осуществляет выполнение перенесенных процессов.