ПОЛИТИКА
информационной безопасности
Ассоциации Российское антидопинговое агентство «РУСАДА»

Версия № 3

1. Назначение.

Настоящая политика вводится для разъяснения основных правил, принципов и ограничений, применяемых в Ассоциации Российское антидопинговое агентство «РУСАДА» (далее – РАА «РУСАДА») с целью минимизации рисков компрометации, несанкционированного уничтожения, изменения, а также хищения конфиденциальной информации, в том числе персональных данных.

2. Цели.

Предотвращение неконтролируемого распространения конфиденциальной информации в результате её разглашения сотрудниками или получения несанкционированного доступа к информации.

Предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации.

Предотвращение несанкционированного доступа к конфиденциальной информации, обеспечение полноты, целостности, достоверности информации.

Обеспечение возможности обработки и использования конфиденциальной информации сотрудниками РАА «РУСАДА», имеющими соответствующие полномочия.

Контроль и учёт информационных ресурсов. Определяет общий порядок обращения с документами, файлами, паролями, доступными информационными ресурсами, содержащими служебную информацию ограниченного распространения.

3. Область применения.

Действие настоящей политики распространяется на всех сотрудников РАА «РУСАДА».

4. Принятые сокращения, термины и определения.

Помимо сокращений РСМК, в настоящей политике также используются следующие определения, сокращения и обозначения:

ЛВС (локальная вычислительная сеть) - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

СКУД (система контроля и управления доступом) - совокупность программно-аппаратных технических средств контроля и средств управления, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.

ПО (программное обеспечение) - программа или множество программ, используемых для управления компьютером.

Удаленный доступ - удаленное подключение к компьютеру с целью управления или просмотра рабочего стола, а также выполнения сопутствующих операций, например, обмен файлами, голосовыми и видео сообщениями и прочее.

RDP - Протокол удаленного рабочего стола (RDP) это проприетарный протокол разработан Microsoft который предоставляет пользователю графический интерфейс для подключения к другому компьютеру через сетевое соединение.

RDP-шлюз – сервер обеспечивающий безопасный канал связи для установки соединения между компьютером клиента и конечным компьютером по протоколу RDP.

РД - Распорядительная документация.

Конфиденциальная информация - сведения конфиденциального характера, доступ к которым ограничен законодательством, в том числе, перечисленные в Перечне сведений конфиденциального характера, утвержденном Указом Президента РФ от 06.03.1997 № 188, в том числе персональные данные, которые обрабатывает РАА «РУСАДА».

Конфиденциальность персональных данных — обязательное требование для соблюдения работниками РАА «РУСАДА», получившими доступ к персональным данным спортсмена (иного лица), не допускать распространения персональных данных без получения предварительного согласия спортсмена (иного лица) или наличия иного законного основания на распространение данной информации в соответствии с Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных» и Всемирного антидопингового кодекса.

Доступ к информации - возможность получения информации и ее использование.

Служебная информация - к служебной информации ограниченного распространения относится информация, касающаяся деятельности РАА «РУСАДА», ограничения на распространение которой диктуются служебной необходимостью.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Защита информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа.

3) реализацию права на доступ к информации.

5. Ответственность

Ответственность за разработку политики возложена на специалиста по информационной безопасности и системному администрированию, который проводит проверку (пересмотр) документа один раз в год, если в течение этого времени в документ не вносились изменения.

Ответственность за применение настоящей политики возлагается на всех сотрудников РАА «РУСАДА».

Настоящая политика доступна для чтения на корпоративном диске РАА «РУСАДА».

6. Права.

Сотрудникам РАА «РУСАДА» разрешается использовать в работе компьютер, мобильные устройства, оргтехнику, выданные работодателем, а также доступные сервисы и сетевые ресурсы организации, предоставленные сотруднику согласно утвержденной Генеральным директором заявке на регистрацию нового пользователя/изменение прав доступа.

В случае возникновения сложностей, при реализации мероприятий, описанных в данной политике, сотрудник может обратиться за помощью, либо консультацией, к специалисту по информационной безопасности и системному администрированию.

7. Обязанности.

7.1 **Пароли.** Доступ к сервисам и в ЛВС организации обеспечивается по средством использования индивидуальных учётных записей, выдаваемых

сотруднику системным администратором. В зависимости от функциональных обязанностей, сотруднику может быть выдано несколько учётных записей. Например: для доступа к ЛВС организации, организации удалённого доступа и подключения к корпоративной сети беспроводного доступа Wi-Fi используются отдельные учётные записи.

Полученные учётные данные должны быть использованы только для подключения к сервису, для которого они предназначены. Пароли должны отличаться и соответствовать требованиям, указанным ниже.

Пользователь обязан своевременно, минимум один раз в три месяца изменять пароль от своей учётной записи, предназначенной для работы в ЛВС РАА «РУСАДА». Пароль от учётной записи пользователя должен соответствовать следующим минимальным требованиям:

- Длинна пароля должна быть не менее 8 (восьми) символов в латинской раскладке клавиатуры.
- В пароле должны быть использованы прописные и строчные буквы, а также цифры. Допускается использование в пароле специальных знаков и символов.
- В пароле не должны использоваться последовательные цепочки цифр, либо букв, а также последовательный набор символов на клавиатуре.
- Пароль не должен содержать никакой личной информации, такой как имена, даты рождения, логины или части этих данных.
- Пароль не должен быть использован повторно, если он использовался ранее.

Запрещается использовать чужие учётные данные для авторизации, входа и использования сервисов РАА «РУСАДА» и ЛВС организации.

Запрещается передавать или сообщать пароль от своей учётной записи ЛВС РАА «РУСАДА», а также пароли от мобильных устройств, ноутбуков и иных сервисов организации, другим сотрудникам или третьим лицам, а также записывать и оставлять их в местах, где они могут быть кем-либо прочитаны и тем самым скомпрометированы.

В случае компрометации пароля, либо подозрений, что пароль может быть скомпрометирован, сотрудник обязан немедленно изменить пароль от своей учётной записи, а также оповестить сотрудника по информационной безопасности об инциденте. В случае невозможности изменить пароль самостоятельно, сотрудник должен сообщить об этом системному администратору.

7.2 Удалённое подключение. Запрещается подключаться к рабочему месту с «чужих» компьютеров, а также устройств, на которых отсутствует, давно не обновлялось, либо работает с ошибками антивирусное ПО.

Категорически запрещается предоставлять кому-либо удалённый доступ к своему рабочему месту/компьютеру/ноутбуку, а также передавать сертификаты, сообщать параметры подключения, логины и пароли доступа.

Запрещается кому-либо передавать компьютер/ноутбук с настроенным удалённым доступом. При необходимости передачи компьютера/ноутбука третьим лицам, должны быть соблюдены условия, обеспечивающие невозможность использования удалённого подключения к рабочему компьютеру посторонними. Сохраненные пароли, сертификаты организации, а также настройки и ярлык для удалённого подключения к рабочему месту/компьютеру/ноутбуку должны быть безвозвратно удалены.

7.3 Программное обеспечение. На рабочих компьютерах, ноутбуках, а также устройствах, выданных сотруднику для выполнения служебных обязанностей разрешается использовать только лицензионное программное обеспечение.

На компьютере/устройстве, которое предоставляется сотруднику для работы, установлено всё необходимое программное обеспечение, указанное в заявке на регистрацию нового пользователя. Установка дополнительного программного обеспечения осуществляется только после согласования с системным администратором.

Запрещается запускать нелицензионное ПО, ПО функционал, которого пользователю до конца не известен, либо может нанести потенциальный вред данным, ЛВС или деятельности организации в целом, а также программы, полученные из недостоверных источников.

7.4 Персональные/конфиденциальные данные. Все документы и внешние носители (флешки, внешние жёсткие диски, CD/DVD и т.п.), содержащие персональные/конфиденциальные данные должны храниться в сейфах или запираемых на замок металлических шкафах, ключи от которых есть только у сотрудников, допущенных к обработке данного рода информации согласно служебным обязанностям. Запрещается оставлять документы, содержащие конфиденциальную информацию в местах, где они могут быть доступны посторонним лицам.

Передача данных, содержащих конфиденциальную информацию, должна осуществляться только по защищённым каналам связи.

В случае, когда гарантировать защищённость канала связи не представляется возможным, файлы, содержащие конфиденциальную информацию, должны быть заархивированы с использованием стойкого алгоритма шифрования и закрыты надёжным паролем (см. п1). Пароль должен передаваться **отдельно** от файла, в другом письме, либо иным способом.

7.5 Хранение файлов. Все документы и другие файлы, используемые в работе, сотрудник обязан хранить на сетевом диске файлового сервера, в своей сетевой папке, папках отдела, к которому прикреплён сотрудник, либо иных сетевых папках, согласованных руководством организации/отдела для хранения данных файлов.

7.6 Использование сети Интернет. Сотруднику разрешается использовать сеть интернет, только в служебных целях. Запрещается посещать подозрительные сайты, у которых отсутствует, просрочен, либо не соответствует имени сайта сертификат. Категорически запрещается предоставлять кому-либо удалённый доступ к компьютеру/ноутбуку, без согласования со специалистом по информационной безопасности и системному администрированию.

Запрещено вводить и указывать, где-либо кроме сетевых ресурсов принадлежащих РАА «РУСАДА», специально предназначенных для этого, учётные данные, полученные для работы с сервисами и ЛВС РАА «РУСАДА».

Запрещается запускать файлы, скачанные из сети Интернет с расширениями несвойственными файлам целевого приложения, а также со сдвоенными расширениями. (Например: для приложений MS Office свойственны расширения: doc, docx, xls, xlsx и т.п.)

7.7 Электронная почта. При получении письма по электронной почте, прежде чем открывать вложения и переходить по ссылкам, указанным в письме, необходимо удостовериться что:

- содержимое поля «отправитель» не вызывает подозрений. Отправитель вам знаком, доменное имя организации вам знакомо, либо данное письмо вы ожидали и т.п.
- вложение имеет расширение свойственное файлам целевого приложения (Например: для приложений MS Office свойственны расширения: doc, docx, xls, xlsx и т.п.)
- у вложения отсутствуют двойные расширения. Расширения указанные последовательно друг за другом (Например: .docx.scr, .xlsx.js и т.п.)

- при наведении курсора мыши на ссылку в подсказке подсвечивается адрес, аналогичный указанному в ссылке, либо соответствующий описанию ссылки (если ссылка в виде текста).
- открыв ссылку, прежде чем совершать какие-либо дальнейшие действия, необходимо убедиться, что в адресной строке браузера указан именно тот ресурс, на который указывала ссылка.
- В случае наличия сомнений или подозрений в недостоверности информации содержащейся в письме, либо в надёжности указанной страницы, необходимо немедленно закрыть страницу и проконсультироваться с системным администратором.

7.8 Внешние носители/накопители информации *(флешки, внешние жёсткие диски и т.д.).* Все внешние носители/накопители информации необходимо проверять на наличие вирусов и вредоносного ПО с помощью установленного на компьютере антивирусного программного обеспечения.

Запрещается подключать к компьютеру внешние накопители, полученные из неизвестных источников. Такие носители должны быть переданы системному администратору для проверки.

7.9 Печать, копирование и сканирование документов. Распечатывая документы, сотрудник должен убедиться в правильности имени выбранного принтера, а также забрать документы из принтера сразу после их распечатки.

Запрещается забирать из принтера чужие документы без согласования с сотрудником, который их распечатал.

При сканировании документов, прежде чем отправить файл, сотрудник должен убедиться в правильности имени выбранного получателя.

Завершив работу по сканированию/копированию документов, сотрудник обязан удостовериться в отсутствии оригиналов документов на стекле/автоподатчике сканирующего устройства, а также убедившись, что МФУ завершил выполнение задания, забрать оригиналы, копии и распечатки документов.

В случае обнаружения оригиналов документов в сканирующем устройстве МФУ, сотрудник должен передать их секретарю.

7.10 Использование ключевых носителей информации. Все носители ключевой и конфиденциальной информации, содержащие ЭЦП, сертификаты и т.д., должны храниться в запираемых на замок металлических шкафах, либо сейфах, доступ к которым имеют только уполномоченные сотрудники.

Запрещается копировать, а также передавать ключевые носители, содержащие конфиденциальную информацию посторонним лицам.

7.11 Мобильные устройства. Запрещается передавать мобильные устройства, а также ноутбуки, третьим лицам. На ноутбуке должен быть установлен сложный пароль (см. п.1), а также антивирусное программное обеспечение.

В случае утери мобильного устройства/ноутбука, сотрудник обязан немедленно информировать специалиста по информационной безопасности и системному администрированию об инциденте.

7.12 Блокировка рабочего компьютера. Покидая своё рабочее место, сотрудник обязан заблокировать компьютер.

7.13 Доступ в помещения. Доступ в арендуемые помещения контролируется СКУД арендодателя. Для прохода в здание и на этажи арендуемые РАА «РУСАДА», сотрудник обязан прислонить индивидуальную магнитную карту (ключ) к считывателю. Использование чужой магнитной карты (ключа) для прохода в помещения офиса – запрещено!

В случае утери магнитной карты (ключа) необходимо **немедленно** сообщить об этом сотруднику по информационной безопасности и системному администрированию, а также ответственному сотруднику отдела управление делами.

Запрещается передавать свою магнитную карту (ключ), другим сотрудникам или третьим лицам, а также пропускать на этаж посторонних. Все гости организации должны сопровождаться ответственными сотрудниками.

Двери на этаж должны быть закрыты. В случае проведения складских работ, перемещения крупногабаритных предметов или иной служебной необходимости, двери, а также дополнительные створки дверных проёмов должны открываться только на время проведения данных работ, а проход должен находиться под контролем сотрудника, ответственного за данные работы.

Ключи от кабинетов находятся на посту охраны при входе в здание. Ключи выдаются сотрудникам РАА «РУСАДА» под роспись в соответствующем журнале. В журнале указывается номер кабинета, точное время, Ф.И.О. сотрудника и подпись. При возврате ключа, в соответствующих колонках отмечается точное время возврата ключа, Ф.И.О. сотрудника и подпись.

Ключи от кабинетов отделов, к которым сотрудник не относится согласно своим должностным обязанностям, разрешается брать только после согласования с руководителем отдела, в ведении которого находится данное помещение, либо генеральным директором организации.

8. Дополнения.

Сотрудники также обязаны изучить и использовать в работе Документированную процедуру управление информационными ресурсами РАА «РУСАДА». Данная процедура доступна для изучения на корпоративном сетевом диске и дополняет Политику по информационной безопасности.