**Защита данных и стандарты безопасности**

**ТОО «BRIF Research Group» (БРИФ Ресеч Груп) (Компания)**

В целях защиты данных и безопасности настоящий документ устанавливает следующие стандарты:

1. **ПОЛИТИКА БЕЗОПАСНОСТИ IT**

Содержит аспекты работы персонала Компании с электронно-вычислительными мощностями, информационными ресурсами и системами сбора, анализа и обработки информации. Помимо прочего регламентирует работу систем безопасности, работу с конфиденциальной и персональной информацией.

# Безопасность работы с ЛВС

ЛВС - локальная вычислительная сеть.

Основной целю организации безопасности пользователей при работе с локальной вычислительной сетью является организация бесперебойной работы локальной вычислительной сети, а также обеспечение информационной безопасности Компании.

Корпоративной локальной вычислительной сетью называется совокупность компьютеров, кабелей, сетевых адаптеров, активного и пассивного сетевого оборудования, работающего под управлением операционных систем и прикладного программного обеспечения.

Локальная корпоративная вычислительная сеть предназначена для:

* Разделения доступа к файлам. Корпоративная ЛВС позволяет многим пользователям работать с одним файлом, хранящимся на центральном файл-сервере.
* Обмен файлами. Корпоративная ЛВС позволяет быстро копировать файлы любого размера с одной рабочей станции пользователя на другую без использования переносных носителей информации.
* Доступа к информации и файлам. Корпоративная ЛВС позволяет запускать прикладные программы с любой из рабочих станций, где бы она ни была расположена.
* Одновременного ввода данных в прикладные программы.
* Разделения принтера. Корпоративная ЛВС позволяет нескольким пользователям на различных рабочих станциях использовать совместно один или несколько принтеров.
* Электронной почты. Возможность использования корпоративной ЛВС в качестве почтовой службы, а именно - рассылка служебных записок, отчетов, докладов, сообщений другим пользователям корпоративной ЛВС.
* Централизованного доступа к сети Internet.

## Регистрация пользователя

Каждый подключенный к сети компьютер должен числиться за пользователем, ответственным за этот компьютер. Информация о пользователе должна заноситься в базу данных домена системным администратором сети.

Регистрация выполняется путем заполнения системным администратором “формы регистрации пользователя”, в которую заносится информация о пользователе, его контактные данные, данные о программном обеспечении, IP-адрес и т.д.

Пользователь обязан хранить свои идентификационные данные (пароли и т.п.) в тайне. Запрещена передача идентификационных данных третьим лицам. Ответственность за все деструктивные действия в ЛВС, произведенные с использованием идентификационных данных пользователя несет владелец идентификационных данных.

При подозрении на то, что идентификационные данные стали известны кому-либо кроме их хозяина, пользователь должен немедленно обратиться к системному администратору с целью их изменения.

При увольнении сотрудником подписывается Обходной лист у Системного Администратора. Учетная запись бывшего сотрудника блокируется. Отдел информационных технологий обеспечивает невозможность доступа уволенного сотрудника к рабочему месту. При необходимости проверяется сохранность и доступность документов и файлов, с которыми работал пользователь, а также его электронной почты.

## Пароли

Пароль должен состоять из не менее чем шести символов и содержать цифры, заглавные и строчные буквы. Недопустимо использование каких-либо слов или комбинаций слов, имен и т.д.

Запрещено записывать пароли на любых носителях.

Пароль должен меняться не реже одного раза в 90 дней.

## Доступ к Internet-ресурсам

Сотрудники имеют доступ к следующим основным видам ресурсов

* HTML-страницам сети Internet,
* электронной почте

Организация и контроль доступа сотрудников регламентируется

* политикой доступа к внешним и внутренним Информационным Системам (ИС)
* оговорёнными исключениями, задокументированными в виде служебных записок и одобренными директором Компании.
* индивидуальными требованиями, предъявляемыми производственной необходимостью.

Контроль производится при помощи корпоративного Proxy-сервера. Любой траффик в обход Proxy категорически запрещён.

Запрещена самовольная организация дополнительных точек доступа в сеть Компании (удаленный доступ, канал по локальной сети) или в сеть Internet (модемный доступ).

Системы удалённого доступа могут устанавливаться только системным администратором с соответствующей регистрацией в документах Компании.

Любые действия в отношении ИС должны быть согласованы с Системным Администратором и одобрены руководством Компании.

## Ограничения и запреты при пользовании Internet-ресурсами

Для нормальной бесперебойной работы ресурсов Internet необходимо строго выполнять следующие ограничения:

Запрещено скачивание видео, аудио, игр, графических и других файлов, не имеющих отношения к текущим служебным обязанностям работника, а также небезопасные исполняемые файлы.

Запрещено посещение и просмотр пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, призывающие к насилию или межнациональной розни).

Запрещено посещение ресурсов трансляции потокового видео и аудио в режиме реального времени (веб-камеры, трансляция телевизионных и музыкальных программ в Internet), игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности Компании, если только это не связано с производственной необходимостью.

Запрещено играть в игры.

Запрещено использование сайтов анонимайзеров, а также программ для анонимного сёрфинга в сети Internet

Запрещено использование программ для зарабатывания денег в сети Internet, таких как Spedia, Web Money и им подобных.

Запрещен хостинг (размещение web-, ftp-сервера) на компьютере пользователя.

Запрещена рассылка информации, носящей рекламный характер (SPAM).

Вся электронная почта, связанная с деятельностью Компании, должна отправляться и приниматься на корпоративный сервер электронной почты. При производственной необходимости использовать электронный адрес, размещенный на сервере в Интернет, должны быть проведены дополнительные мероприятия по обеспечению безопасности и конфиденциальности информации.

Запрещено использование внешних почтовых ящиков (mail.ru, gmail.com, hotmail.com, yandex.kz и т.д.).

Информация о посещенных пользователем ресурсах Internet протоколируется. Отчеты о входящем трафике пользователя могут быть востребованы Администрацией Компании для ознакомления в любое время без уведомления пользователя.

Сайты с сомнительным содержанием или ресурсы, не имеющие прямого отношения к деятельности фирмы, заносятся в “черный список” и в дальнейшем доступ к будет ним закрыт.

Системный администратор вправе закрыть любой Интернет-ресурс без предупреждения пользователей в целях информационной безопасности.

## Ограничения и запреты при пользовании Электронной почты (E-Mail)

Основной задачей Электронной почты является оперативная связь сотрудников с клиентами, подрядчиками, пересылка документов, отчетов и прочих файлов, отражающих деятельность или деятельность пользователя.

Электронная переписка посредством корпоративных почтовых адресов является официальным документооборотом Компании.

 В связи с чем по электронной почте запрещена пересылка:

* сообщений и содержимого личного характера;
* вложений из внешних непроверенных источников;
* информации, не связанной с профессиональной деятельностью или интересами фирмы;
* содержимое расистского, экстремистского и уголовного характера;
* отправка электронных писем и других сообщений, содержащих вложенные файлы, имеющих значительный объем (более 15 Mb), без предварительного согласования с системным администратором.

В переписке следует соблюдать этику и уважение к собеседнику.

Следует проявить особую бдительность с входящей электронной почтой.

 Запрещено прочтение электронной почты, содержащей вложенный файл, пришедшей от неизвестных лиц или с рекламной рассылкой.

Типы файлов, которые никогда не нужно открывать:

\*.avi, \*.asf, \*.ade, \*.adp, \*.asx, \*.bas, \*.bat, \*.cfg, \*.chm, \*.cmd, \*.com, \*.cpl, \*.crt, \*.exe, \*.gif, \*.hlp, \*.hta, \*.inf, \*.ins, \*.isp, \*.js, \*.jse, \*.htm, \*.lnk, \*.mdb, \*.mpeg, \*.mp3, \*.mde, \*.mmf, \*.msc, \*.msi, \*.msp, \*.mst, \*.pcd, \*.php, \*.pif, \*.prf, \*.reg, \*.scf, \*.scr, \*.sct, \*.shb, \*.shs, \*.swf, \*.url, \*.vb, \*.vbe, \*.vbs, \*.wsc, \*.wsf, \*.wsh.

При получении от делового партнера несвойственное для него послания (на английском/испанском/немецком языке, либо содержащее музыку/порно/скринсэйвер) немедленно обратитесь к системному администратору и не предпринимайте никаких самостоятельных действий.

Вся почта автоматически проверяется на наличие вирусов в письме и вложенных файлах. При невозможности безопасного удаления или лечения вируса, письмо и (или) вложенные файлы могут быть автоматически удалены.

Запрещено публиковать личный электронный адрес на досках объявлений, в конференциях, гостевых книгах, а также при регистрации на сторонних сайтах.

Запрещено сообщать лицам, не работающим в Компании, любые групповые электронные адреса (all@, PPMService@ или PPMStaff@).

 Запрещена массовая рассылка сообщений посредством электронной почты и других средств персонального обмена информацией (включая службы немедленной доставки сообщений) иначе как по явно и недвусмысленно выраженной инициативе получателей:

- электронных писем и других сообщений (в том числе единичных) рекламного, коммерческого или агитационного характера;

- писем и сообщений, содержащих грубые и оскорбительные выражения и предложения;

- рассылка сообщений, содержащих просьбу переслать данное сообщение по цепочке другим пользователям (chain letters, письма «счастья»);

- использование корпоративных групповых адресов иначе, как по их прямому назначению, установленному владельцем адресов и/или стандартами.

- писем множеству пользователей, содержащие аудио, видео, графические, текстовые файлы развлекательного характера.

Запрещено открывать на локальном компьютере прикреплённые файлы, документы к почте из непроверенных источников без предварительного сохранения их на локальном жестком диске для последующей автоматической проверки антивирусной программой.

Запрещено переходить по ссылкам, ведущим на сайты в Internet, полученных с помощью почтовых сообщений (за исключением списка одобренного департаментом безопасности и отделом IT).

Запрещена подписка на новости и иные массовые рассылки на именные корпоративные электронные адреса.

Запрещено фальсифицировать адрес отправителя, подключаться к почтовому серверу иначе как почтовым клиентом.

Запрещены попытки взлома, перебора, перехвата пароля чужих учётных записей для чтения, отправки, удаления почтовых сообщений других пользователей.

Вся входящая и исходящая почта сотрудника может быть просмотрена без его уведомления назначенными сотрудниками отдела информационных технологий по указанию руководства.

## Обязанности пользователя при работе с Локальной сетью

 Запрещены любые попытки деструктивных действий по отношению к нормальной работе Компании.

 Запрещено использование программ (различные трасерты, сниферы, сканеры портов), осуществляющих сканирование узлов, серверов или любых элементов с целью выявления внутренней структуры сети, списков открытых портов.

 Запрещена установка дополнительных сетевых протоколов, изменение конфигурации настроек сетевых интерфейсов.

 Запрещен просмотр видео через сеть. За исключением случаев, связанных со служебной необходимостью.

 Запрещено открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на переносных носителях без предварительного сохранения на локальном жестком диске и последующей автоматической проверки антивирусной программой.

 Запрещено осуществление попыток несанкционированного доступа к ресурсам сети, проведение сетевых атак и сетевого взлома и участие в них, для последующего использования такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю. Под несанкционированным доступом понимается любой доступ способом, отличным от предлагавшегося владельцем ресурса.

 Запрещена передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

# Безопасность работы с системами доставки сообщений

## Общие принципы

К Системам Доставки Сообщений (СДС) относятся:

 -мессенджеры (WhatsApp, Telegram, Viber и т.д);
 -системы видеоконференций (Skype, Google Meet, Телемост и т.д.);
 -системы онлайн чатов (YouTube Stream);
 -переписка в любом виде в социльных сетях.

На современном этапе большинство СДС носят гибридный характер, а так же могут являться частью более крупного пакета ПО. Таким примером может быть Microsoft Teams.

## Правила использования

 По умолчанию сотруднику запрещено использовать ЛЮБЫЕ СДС на рабочем месте кроме Корпоративной Электронной Почты. Ограничение касается как Desktop так и Web-версии приложений.

 Установка и использование возможны только для производственной необходимости и с разрешения руководителя Компании при условии соблюдения остальных норм настоящего документа.

# Безопасность пользования рабочей станцией

 Рабочая станция является неотъемлемой частью современного рабочего места сотрудника. Рабочая станция состоит из персонального компьютера (ПК), одного или нескольких мониторов, переферийного оборудования (принтеры, модемы, USB устройства и т.д.), систем ввода информации (клавиатура, мышь, сканер штрих-кодов, сканер изображений, веб-камера и т.д.). Рабочая станция может функционировать как в рамках сети (online), так и автономно (offline).

 Так же следует отметить рабочую станцию без собственных вычислительных мощностей (терминал), и виртуальное рабочее место (Удалённый рабочий стол).

 Изложенная ниже политика применима ко всем перечисленным типам рабочих мест.

## Основные правила эксплуатации рабочей станции

 Сотрудник обязан бережно относиться к выделенному ему рабочему месту. Не допускать порчи как намеренной так и случайной. Не допускать к рабочему месту лиц без соответсвующего права на эксплуатацию или обслуживание. В случае подобного инцидента следует незамедлительно проинформировать своего непосредственного руководителя.

 Современная техника не подразумевает ремонт оборудования силами самого сотрудника. В случае поломки или подозрения на некорректную работу следует незамедлительно оповестить департамент IT и своего непосредственного руководителя.

 Оповещение должно быть в виде электронного письма-заявки в установленной форме на адрес системного администратора.

## Аппаратная часть рабочей станции.

 Сотруднику категорически запрещено самостоятельно изменять конфигурацию оборудования. В случае производственной необходимости подаётся заявка на адрес системного администратора в установленной форме. Заявка дублируется на почтовый ящик руководителя направления.

 Запрещено использование личных устройств на рабочем месте. В случае производственной необходимости или в рамках нестандартных потребностей сотрудника, Компания может пойти на исключения. Однако использование подобного оборудования должно быть согласовано с департаментом IT и не нести угрозы безопасности, технологическим процессам, здоровью других сотрудников.

 На рабочих станциях Компании запрещено использование USB и CD накопителей. В случае потребности сотрудника записать\прочитать данные с USB или CD накопителей, сотрдуник обязан обратиться за помощью к системному администратору.

 Все операции симстемного администратора с USB и CD носителями в обязательном порядке записываются в журнал. Данные этого журнала используются в случае разбора инцидентов преднамеренного или случайного несанкционированного распространения информации.

## Программная часть рабочей станции

 Под программной частью подразумевается Операционная система и любые прикладные программы и сервисы установленные на рабочую станию.

 Все рабочие станции настроены в рамках одной из моделей конфигурации.

 Сотруднику категорически запрещено самостоятельно устанавливать, удалять или иным образом изменять программное обеспечение на рабочей станции, даже в случае если данная опция не заблокирована политиками домена или отдельно-стоящего устройства. Под данное ограничение попадают так же ВСЕ иные корпоративные электронные устройства (Планшеты, Смартфоны, Треккеры и т.п.).

 В случае необходимости изменения конфигурации подаётся заявка на адрес системного администратора в установленной форме. Заявка дублируется на почтовый ящик руководителя направления.

 Вне зависимости от потребностей и производственной необходимости, на рабочие станции запрещено устанавливать: нелицензионное ПО, «взломанное» ПО, ПО с подозрительной активностью (даже в том случае если антивирус не блокирует его работу), ПО любой религиозной, экстремисткой, политической направленности.

## Рабочая информация на персональной рабочей станции

 ЛЮБАЯ информация, находящаяся на рабочей станции является корпоративной собственностью Компании (если обратное не определено договором или иным документом).

 Вся рабочая информация должна храниться в строго отведённом месте, иметь резервные копии (полные и/или разностные). Метод хранения и доступность информации должен строго подчиняться политике доступа к внешним и внутренним тнформационным системам.

 Использование общих сетевых хранилищ должно быть сведено к минимуму. Общие хранилища должны регулярно очищаться и мониториться на предмет публикации персональных данных.

 Любые файлы, не имеющие отношение к деятельности Компании (видео, аудио, графические файлы, игры и др.), и сохраненные на любых корпоративных ресурсах, могут быть удалены без предупреждения.

Для передачи информации между отделами или пользователями существует папка «Public».

 Папка «Public» используется только для временного хранения какой-либо информации, для её передачи между пользователями. После передачи информации или ее использования файлы необходимо удалить незамедлительно.

 Запрещено защищать документы, относящиеся к деятельности Компании паролем. При необходимости ограничения доступа к документам, следует обращаться к сотрудникам отдела информационных технологий.

 Все операции пользователя с файлами, расположенными на файловом сервере, в обязательном порядке записываются в журнал. Данные этого журнала используются в случае разбора инцидентов преднамеренного или случайного удаления документов или изменения информации.

## Блокировка и отключение компьютера при завершении работы

 Пользователь обязуется блокировать свой рабочий компьютер каждый раз при его отсутствии на рабочем месте. Для этого необходимо нажать одновременно клавиши СТRL + ALT + DEL и выбрать Lock Computer(Блокировка).

 После завершения рабочего дня пользователь обязуется выключать свой компьютер (если иное не предусматривает производственный процесс).

Ответственность за неисполнение правил и политик

 Неисполнение обязанностей и процедур действующей политики, приведшее к каким-либо негативным последствиям, влечет за собой применение мер дисциплинарной и гражданско-правовой ответственности.

 Применение мер ответственности инициируется направлением «Служебного письма» на имя руководителя отдела, в штатном расписании которого состоит «нарушитель». Служебное письмо может быть направлено от имени и за подписью Директора по информационным технологиям.

 Подача «Служебного письма» требует от «нарушителя» предоставления «Объяснительной записки» о причинах нарушения. При отсутствии оправдательных документов и в случае, если содержание объяснительной записки будет неубедительным, к сотруднику все равно могут быть применены вышеуказанные меры ответственности.

 Обязанностью руководителей отделов является уведомление Директора по информационным технологиям о принятых мерах в отношении «нарушителя» (направление копии приказа о дисциплинарном взыскании).

1. **ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Настоящая политика обработки персональных данных основана на Законе Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных Компании.

* 1. Компания ставит своей важнейшей целью и условием осуществления своей деятельности соблюдение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
	2. Настоящая политика Компании в отношении обработки персональных данных применяется ко всей информации, которую Компания может получить о посетителях своего веб-сайта, а так же респондентах участвующих в исследованиях проводимых Компанией.

## Основные понятия, используемые в политике

* 1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
	2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
	3. Веб-сайт – совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети интернет по сетевому адресу Компании;
	4. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;
	5. Обезличивание персональных данных — действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному Пользователю или иному субъекту персональных данных;
	6. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
	7. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому Пользователю веб-сайта Компании;
	8. Пользователь – любой посетитель веб-сайта Компании;
	9. Респондент – любое лицо, участвующее в исследованиях Компании, как лично, так и через законного представителя (либо с согласия такового);
	10. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
	11. Распространение персональных данных – любые действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
	12. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;
	13. Уничтожение персональных данных – любые действия, в результате которых персональные данные уничтожаются безвозвратно с невозможностью дальнейшего восстановления содержания персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

## Список обрабатываемых данных

Компания может обрабатывать следующие персональные данные Пользователя и/или Респондента:

* + Фамилия, имя, отчество;
	+ Электронный адрес и адрес прописки/проживания;
	+ Номера телефонов;
	+ Также на сайте происходит сбор и обработка обезличенных данных о посетителях (в т.ч. файлов «cookie») с помощью сервисов интернет-статистики;
	+ Вышеперечисленные данные далее по тексту политики объединены общим понятием Персональные данные.

## Цели обработки персональных данных

* + Цель обработки персональных данных Пользователя и/или Респондента — информирование Пользователя и/или Респондента посредством отправки электронных писем.
	+ Также Компания имеет право направлять Пользователю и/или Респонденту уведомления о новых продуктах и услугах, специальных предложениях и различных событиях. Пользователь всегда может отказаться от получения информационных сообщений, направив Компании письмо с пометкой «Отказ от уведомлениях о новых продуктах и услугах и специальных предложениях».
	+ Обезличенные данные Пользователей и/или Респондентов, собираемые с помощью сервисов интернет-статистики, служат для сбора информации о действиях Пользователей и/или Респондентов на сайте, улучшения качества сайта и его содержания.

## Правовые основания обработки персональных данных

* + Компания обрабатывает персональные данные Пользователя и/или Респондента только в случае их заполнения и/или отправки Пользователем и/или Респондентом самостоятельно через специальные формы, расположенные на Компании, так и получаемые от интервьюеров либо других работников Компании. Заполняя соответствующие формы и/или отправляя свои персональные Компании, Пользователь и/или Респондент выражает свое согласие с данной политикой.
	+ Компани обрабатывает обезличенные данные о Пользователе и/или Респонденте в случае, если это разрешено в настройках браузера Пользователя (включено сохранение файлов «cookie» и использование технологии JavaScript).

## Порядок сбора, хранения, передачи и других видов обработки персональных данных

* + Безопасность персональных данных, которые обрабатываются Компанией, обеспечивается путем реализации правовых, организационных и технических мер, необходимых для выполнения в полном объеме требований действующего законодательства в области защиты персональных данных.
	+ Компания обеспечивает сохранность персональных данных и принимает все возможные меры, исключающие доступ к персональным данным неуполномоченных лиц.
	+ Персональные данные Пользователя и/или Респондента никогда, ни при каких условиях не будут переданы третьим лицам, за исключением случаев, связанных с исполнением действующего законодательства.
	+ В случае выявления неточностей в персональных данных, Пользователь может актуализировать их самостоятельно, путем направления Компании уведомление на адрес электронной почты с пометкой «Актуализация персональных данных».
	+ Срок обработки персональных данных является неограниченным. Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Компании уведомление посредством электронной почты на электронный адрес Компании с пометкой «Отзыв согласия на обработку персональных данных».

## Трансграничная передача персональных данных

* + Компания до начала осуществления трансграничной передачи персональных данных обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается надежная защита прав субъектов персональных данных.
	+ Трансграничная передача персональных данных на территории иностранных государств, не отвечающих вышеуказанным требованиям, может осуществляться только в случае наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных и/или исполнения договора, стороной которого является субъект персональных данных.

## Заключительные положения

* + Пользователь может получить любые разъяснения по интересующим вопросам, касающимся обработки его персональных данных, обратившись к Компании с помощью ее электронной почты.
	+ В данном документе будут отражены любые изменения политики обработки персональных данных Компании. Политика действует бессрочно до замены ее новой версией.
1. **ПОЛИТИКА ДОСТУПА К ВНЕШНИМ И ВНУТРЕННИМ ИНФОРМАЦИОННЫМ СИСТЕМАМ**

# Цель:

Минимизировать вероятность нарушения конфиденциальности информации путём разграничения доступа к внутренним и к внешним ресурсам.

# Области действия:

* + Физическая: рабочие помещения Копании, корпоративные устройства, носители информации.
	+ Логическая: локальные папки, установленные на персональном компьютере (ПК) утилиты, локальные и внешние сайты.

# Основополагающие принципы и понятия:

Информационная система (ИС) – совокупность физических и электронных носителей, использующихся для хранения и обработки информации.

Третье лицо – лицо, не аффилированное с Компанией и не имеющее прав на просмотр и использование корпоративной информации.

Корпоративное устройство – устройство, имеющееся в собственности компании.

Служебное помещение – помещение, в котором располагаются корпоративные устройства и/или сотрудники Компании.

Принцип 1: Доступ к любым ИС сотрудником Компании должен быть минимально необходимым и достаточным для выполнения последним его прямых служебных обязанностей.

Принцип 2: политика должна предусматривать разграничения доступа как к физическим, так и к электронным ресурсам.

Принцип 3: Обеспечение сотрудникам доступа к ИС должно осуществляться с использованием ролевого разграничения доступа с присвоением разрешений и запретов каждой роли.

Данные, доступ к которым должен быть ограничен:

* Электронные письма и вложения к ним
* Базы данных и/или онлайн-системы, облачные хранилища
* Социальные сети и другие средства массовой коммуникации
* Сайты, например, онлайн-каталоги сотрудников
* Данные опросов и исследований
* Системы видеонаблюдения и объекты с физическим доступом (например, данные, хранящиеся на электронных ключах, отслеживание местоположения и т. п.)
* Бумажные документы, такие как договоры с сотрудниками и клиентами, письма, служебные записки, отчеты и фотографии (например, офисные бейджи, пропуска, личные дела сотрудников)

# Правила:

## Физическая область действия.

Обеспечение безопасности в физической области действия данной политики включает в себя контроль служебных помещений, учёт и поддержание работоспособности корпоративных устройств и внешних носителей информации Компании, а также обеспечение целостности, доступности и конфиденциальности данных на них путём соблюдения следующих правил:

* 1. Доступ в служебные помещения должен осуществляться при помощи индивидуальных карт-пропусков (ИКП), имеющихся у каждого сотрудника Компании.
	2. Третьи лица не должны иметь доступ в служебные помещения Компании.
	3. Сотрудники Компании не должны передавать свои ИКП либо самостоятельно предоставлять доступ в служебное помещение третьим лицам.
	4. Третьи лица не должны иметь физический доступ к корпоративным устройствам Компании
	5. Служебные помещения должны быть оснащены камерами наблюдения, ведущими запись в реальном времени.
	6. Все корпоративные устройства и данные на них должны быть защищены паролем, шифром или иным способом.
	7. Сотрудники Компании не должны иметь доступа к ПК других сотрудников и к информации на нём.
	8. Сотрудник Компании не должен иметь доступа к корпоративным устройствам Компании и информации на них, если это не затрагивает его профессиональную деятельность.
	9. Все внешние носители информации Компании и данные на них должны быть защищены паролем, шифром или иным способом.
	10. Третьи лица не должны иметь доступ к внешним носителям информации Компании.

## Логическая область действия.

Обеспечение безопасности в логической области действия данной политики включает в себя разграничение доступа к информации на электронных носителях и устройствах, а также запреты и разрешение на использование различных Интернет-ресурсов.

* 1. Сотрудники Компании не должны передавать известные им пароли от корпоративных устройств и приложений (ПК, Базы данных, Почта, Мобильные устройства и т.д.).
	2. Сотрудники Компании не должны предоставлять доступ к корпоративным данным субъектам, не имеющим прав на просмотр и использование этих данных.
	3. Права на доступ к данным определяются регламентами Компании, политикой безопасности, и прямыми директивами уполномоченных лиц.
	4. Каждый сотрудник обязан вести корпоративную переписку используя только корпоративный почтовый ящик. Вся информация, передаваемая и получаемая через переписку, является конфиденциальной и защищена от разглашения законодательством.
	5. Доступ к базам данных (БД) Компании должен осуществляться через специализированные аккаунты.
	6. При создании корпоративного приложения и/или веб-интерфейса с подключением к БД должен использоваться специально предназначенный для этого аккаунт с ограниченным набором разрешенных действий.
	7. Сотрудники Компании не имеют права пользоваться социальными сетями/мессенджерами/другими средствами массовой коммуникации.
	8. Внутренние сайты Компании должны быть доступны только внутри локальной сети.
	9. Доступ к данным, расположенным на локальных сайтах Компании, должен разграничиваться путём создания пользовательских аккаунтов для локальных сайтов.
	10. Проведение социальных исследований и/или опросов с получением персональных данных должно проводиться в рамках законодательства.
	11. Доступ к системе видеонаблюдения и её записям должен быть только у уполномоченного сотрудника.
1. **ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ**

Компания и ее сотрудники стремятся к ответственному сбору, управлению, использованию и защите данных. Эта политика применяется ко всем работникам и подрядчикам, которые обрабатывают данные и личную информацию или используют информационные системы компании.
Личная информация - это любая информация или мнение, относящиеся к определенным лицам в том числе имя, адрес, номер телефона, адрес электронной почты (включая рабочий адрес электронной почты), национальный идентификационный номер или другие такие идентификаторы. Источники личной информации значительно различаются, и включают в себя:

* электронная почта и вложения;
* базы данных и / или интернет-системы, содержащие личную информацию, социальные медиа или другие средства массовой коммуникации и т.д;
* сайты - интернет-каталоги работника, онлайн сборщики данных и т.д;
* CCTV и физический доступ к сайтам через электронные ключи, отслеживание местоположения и т.д;
* бумажные документы – контракты сотрудников и клиентов, письма, напоминания, отчёты и т.д.;
* фотографии - офисные значки, пропуска, записи о сотрудниках и т.д.

Некоторые клиентские контракты могут включать в себя определенные персональные данные, относящиеся к клиенту, и которые шире, чем юридические определения Компании. Операционные компании должны работать в тесном контакте с клиентами, чтобы гарантировать, что личная информация обрабатывается и защищается и согласуется с договором.

Конфиденциальность данных - это:

* защита персональной информации – ограниченный доступ и шифрование данных;
* персональная информация собирается и отсылается в защищенном виде согласно законодательству;
* система разумных процессов для предотвращения распространения, использования или доступа к личной информации без законных оснований. Это, как правило, но не всегда индивидуальные соглашения; а также равновесие между информацией в общем доступе при одновременной защите персональной информации и идентификаторов.

Соблюдение законодательства

Компания стремится к соответствию применяемым законам и нормам конфиденциальности и защиты данных, нормативным актам и договорам.

Клиенты

Компания работает с множеством контрагентов. Контрагенты должны понимать, что эти термины означают и как они влияют на наши существующие технологические инфраструктуры. Мы также должны понимать последствия этих терминов при подготовке предложений о новых исследовательских методах, маркетинге, цифровых приложениях или других продуктах для клиентов, которые включают персональную информацию.

Потребители

Мы всегда общаемся с потребителями в допустимом порядке. Нормы допустимости варьируются в зависимости от страны, и Компания должна быть осведомлена о юридических требованиях. "Допустимое" может означать своевременное информирование клиентов/респондентов, где хранится их информация, кто может получить доступ к ней и как она используется. В некоторых случаях законодательство требует получения определенных типов согласия от клиента/респондента, и это является обязанностью Компании гарантировать соблюдение правовых обязательств.

Управление данными

Для более эффективной работы Компания консолидируем личную информацию от имени наших сотрудников (например, централизованная HR система) и наших клиентов (например, доступ к системам управления взаимоотношениями с клиентами и / или потребительские данные, собранные для прямого маркетинга, центров обработки вызовов или маркетинговых исследований).

## Политика и осведомленность

Компания должна осуществлять справедливые и разумные политики конфиденциальности и процедуры и приводить их в действие.

Компания должна знать законы, включая те, которые относятся к государственным контрактам, и осуществить необходимые процедуры. Условия действующего законодательства должно проводиться в договоры, иные внутренние бизнес-процессы и системы.

## Безопасность

Компания должна иметь разумные, актуальные меры контроля для предотвращения несанкционированного доступа к сайтам и системам.

Компания должна соответствовать ИТ-политике и политике безопасности и принять разумные и практические меры для обеспечения конфиденциальности, целостности и доступности личной информации.

Должны быть рассмотрены следующие меры защиты:

* соответствующее ограничение и защита (включая шифрование) личной информации, хранящейся на мобильных вычислительных устройствах и оборудовании, в том числе, но не ограничиваясь, ноутбуки, КПК, карты памяти, CD-ROM и мобильные телефоны;
* предотвращение несанкционированного удаленного и локального доступа к системам хранения личных данных, документирование, где это применимо, использование межсетевых экранов, антивирусного программного обеспечения,
внесение исправлений и управление учетной записью пользователя;
* предотвращение несанкционированного физического доступа к системам хранения личной информации, документирование, где это применимо, контроль доступа, относящиеся к серверным помещениям, документам HR и финансовым данным, данным клиента и физического доступа к сайтам;
* предотвращение передачи личной информации неуполномоченным лицам или
группам, включая клиента и передачи данных внутри компании, и особенно передача личной информации через государственные границы.

## Хранение личной информации

Вся личная информация должна храниться в соответствии с политикой компании и минимальным разрешенным сроком хранения. Смотрите

## Удаление личной информации

Любая личная информация, которая больше не нужна и / или попадает под действующее законодательство/ либо указан конкретный срок её использования должна быть утилизирована на безопасной и конфиденциальной основе.

## Передача личной информации

Данные часто передаются поставщикам для предоставления услуг клиентам и сотрудникам. Компания должна убедиться, что передача действительно необходима для бизнеса, и предполагает большие преимущества в выполнении определенного контракта клиента

Соответствующие методы и протоколы надежности должны соблюдаться при передаче личной информации. Адекватные меры безопасности помогут уменьшить нарушения, потери и несанкционированный доступ третьих лиц.