Приложение 9
к распоряжению Администрации
городского округа Химки
Московской области
от 30.09.2021 № 56-р

ПРОЕКТ РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА К СЕГМЕНТУ ЕИСОУ

«УТВЕРЖДАЮ»

_____
(наименование должности, фамилия, инициалы)

_____
печать
«____» _____ 20__ года

ЕДИНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ОКАЗАНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ

МОСКОВСКОЙ ОБЛАСТИ

(ЕИСОУ)

РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА

К СЕГМЕНТУ ЕИСОУ

_____

(наименование организации)

ОГЛАВЛЕНИЕ

Общие положения

Настоящий документ устанавливает правила доступа работников _____ к персональным данным, содержащимся в Сегменте Единой информационной системе оказания государственных и муниципальных услуг московской области (далее – персональные данные).

В настоящем документе используются следующие основные понятия:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

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 (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Информационные ресурсы, содержащие персональные данные – отдельные документы и массивы документов, а также документы и массивы документов в информационных системах (банках данных, архивах), доступ к которым ограничен в соответствии с действующим законодательством и локальными нормативными документами, и которые содержат персональные данные.

Доступ пользователя к информационным ресурсам – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Порядок предоставления доступа к информационным ресурсам

Предоставление доступа работникам к любым информационным ресурсам осуществляется в соответствии с правилами и регламентами, действующими в _____.

Перед предоставлением работнику доступа к информационным ресурсам, содержащим персональные данные, необходимо:

1. Предусматривать в разделе «обязанности работника» в трудовом договоре условия об обязанности работника не разглашать сведения, составляющие государственную и иную охраняемую федеральными законами тайну, а также сведения, ставшие ему известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство и соблюдать требования локальных нормативных актов, регулирующих порядок обращения с персональными данными.

2. Ознакомить работника под подпись со следующими документами:

- Перечень защищаемых информационных ресурсов Сегмента;
- Инструкция по обеспечению безопасности обрабатываемых персональных данных;
- Инструкция пользователя Сегмента ЕИСОУ.

На основании решения руководителя организации (в случае необходимости) и руководителей структурных подразделений (подразделения работника и подразделения, располагающего ресурсами, к которым необходим допуск) осуществляется допуск пользователя к персональным данным, в объеме, необходимом для выполнения им своих функциональных обязанностей.

При переводе на другую должность основанием для допуска служит приказ/распоряжение о переводе. В этом случае допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.

Перечень защищаемых информационных ресурсов необходимо держать в актуальном состоянии.

Порядок прекращения доступа к информационным ресурсам

Прекращение предоставления доступа пользователям к персональным данным осуществляется в следующих случаях:

- увольнение сотрудника;
- перевод сотрудника на другую должность, не предусматривающую необходимости доступа к защищаемым ресурсам;
- компрометация аутентификационных данных пользователя либо нарушение пользователем требований информационной безопасности.

В случае компрометации аутентификационных данных пользователя начальник подразделения извещает в письменном виде администратора информационной безопасности о факте компрометации. Администратор информационной безопасности должен уведомить в письменном виде ответственного за ресурс и лицо, выполняющее функции системного администратора, о необходимости отключения доступа пользователя к ресурсу и инициировать служебное расследование.

Контроль доступа к информационным ресурсам

Контроль правомерности предоставления доступа пользователей к информационным ресурсам возлагается на администратора информационной безопасности в соответствии с инструкцией администратора информационной безопасности Сегмента ЕИСОУ.

Для осуществления контроля правомерности предоставления доступа пользователей к информационным ресурсам администратор информационной безопасности ведёт журнал предоставления доступа (Приложение 1).

Ответственность

Работники, допущенные к работе с персональными данными, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность за разглашение персональных данных в соответствии с законодательством Российской Федерации, а также материальную ответственность за нарушение установленных в организации требований по защите персональных данных.

Приложение 1

Журнал
предоставления доступа пользователей к информационным ресурсам

№ п/п	Наименование (тип) ресурса (включая установленное программное обеспечение)	Должность	Ф.И.О.	Примечание

Приложение 2

Разрешительная система доступа к информационным (программным) ресурсам:

№ п/п	Наименование (тип) ресурса	Категория защищаемого ресурса	Место хранения защищаемого ресурса	Права пользователей по доступу к информации	
				Пользователь	Администратор
1	Документы, разрабатываемые пользователями	ПДн	C:\User C:\AIS_APP	RWAD	-
			C:\Admin	-	RWAD
2	Средства настройки и управления СЗИ от НСД, пароли доступа пользователей и администратора безопасности	Служебная информация	C:____	R	RWAD
3	Основные конфигурационные файлы ОС и драйверы СЗИ от НСД	Служебная информация	C:____, C:\Windows	R	RWAD

R – читать; A – добавлять (создавать) файлы;

W – записывать; D – удалять файлы.

Отметка об ознакомлении пользователя с нормативными документами по информационной безопасности:

- Перечень защищаемых информационных ресурсов Сегмента ЕИСОУ;
- Положение о порядке организации и проведения работ по защите персональных данных;
- Инструкция пользователя Сегмента ЕИСОУ.

№ п/п	Ф.И.О.	Дата	Подпись