**ПОРЯДОК доступа сотрудников в помещения, где ведется обработка персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок доступа сотрудников МБДОУ ЦРР ДС№33 п. Новый в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с требованиями Федерального закона ‑ФЗ «О персональных данных», постановления Правительства РФ «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановления Правительства РФ «Об утверждении «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в целях обеспечения защиты конфиденциальной информации, обрабатываемой в МБДОУ ЦРР ДС№33 п. Новый, и исключения фактов неконтролируемого пребывания в них посторонних лиц.  Настоящим документом определяются границы контролируемой зоны, порядок доступа в неё работников и посетителей, а также правила обработки и хранения документов, содержащих персональные данные, и материальных носителей персональных данных.Порядок устанавливает единые требования к обеспечению сохранности технических средств и персональных данных.

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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.Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники. Неавтоматизированная обработка персональных данных – обработка персональных данных без использования средств вычислительной техники. Технические средства – серверные станции, персональные компьютеры и ноутбуки, настроенные на доступ к программному обеспечению, хранящему и обрабатывающему персональные данные сотрудников и контрагентов. Контролируемая зона (КЗ) ­– территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска. Постоянная контролируемая зона – это зона, границы которой устанавливаются на длительный срок. Временная контролируемая зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

3. ГРАНИЦЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

3.1. Границы контролируемых зон объектов утверждаются приказом заведующего. Граница контролируемой зоны ДОУ ограничивается периметром здания.

3.2. В выделенных на схеме помещениях, определенных в соответствии с функциональными обязанностями должностных лиц, обрабатывающих персональные данные, приняты организационные меры по ограничению несанкционированного доступа к информации ограниченного распространения.

3.3. Контроль доступа на территорию контролируемой зоны объекта ДОУ осуществляется в соответствии с разработанными внутренними нормативами и организационно-распорядительными документами.

3.4. При необходимости, в целях обеспечения защиты конфиденциальной информации за пределами постоянной контролируемой зоны и обеспечения санкционированного (контролируемого) пребывания в ней посторонних лиц, в организации может быть организована временная контролируемая зона. Границы временной контролируемой зоны определяются, исходя из целей планируемого мероприятия, на основании принятых нормативных документов и выполнения режимных мер.

4. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

4.1. В целях обеспечения сохранности технических средств и материальных носителей помещения, в которых осуществляется обработка персональных данных,  оборудованы охранной и пожарной сигнализацией, а также прочными дверями. Ключи от замков передаются и находятся на ответственном хранении у сотрудников ДОУ, работающих в служебных помещениях, а также у сотрудника, уполномоченного хранить резервные ключи от замков всех помещений.

4.2. В случае, если в течение рабочего дня сотрудник отдела уходит из помещения, он обязан проследить, чтобы в помещении не было посторонних лиц и закрыть помещение на замок.

4.4. По окончании рабочего дня помещения, в которых осуществляется обработка персональных данных, после запирания сдаются

4.5. Нахождение посторонних лиц в помещениях, где осуществляется обработка персональных данных, допускается только в присутствии сотрудников ДОУ, непосредственно работающих в данном помещении,  с соблюдением установленных правил ограничения доступа к обрабатываемой информации.

5. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

5.1. Закрытие помещений, в которых осуществляется обработка персональных данных, производится ответственными работниками по окончании рабочего времени, проведения в нём (при необходимости) влажной уборки и осмотра его в целях выявления и устранения возможных нарушений (не выключенное оборудование, неубранные документы, незапертые хранилища, окна и т. п.), в том числе правил противопожарной безопасности (отключение электрических приборов, освещения и т. п.).

5.2. После осмотра помещения, выявления и устранения недостатков, ответственный сотрудник закрывает помещение, передаёт его установленным порядком под охрану сторожа. С указанного момента помещение считается принятым под охрану.

5.3. При входе в помещения, в которых осуществляется обработка персональных данных, ответственный работник производит внешний осмотр на предмет выявления возможных видимых недостатков (отсутствие техники, оборудования) и нарушений (повреждение целостности дверей и т. п.). При отсутствии признаков нарушения целостности охраняемого объекта или причинения ущерба объект считается снятым с охраны.

5.4. В случае обнаружения повреждения (нарушения целостности) внешней двери помещения, в котором осуществляется обработка персональных данных,  или при обнаружении попытки проникновения в него ответственный работник незамедлительно сообщает о случившемся, после чего должностное лицо принимает необходимые меры по локализации нарушения:

- вызывает сотрудников полиции по номеру 02 или мобильному 112 для принятия мер реагирования;

- в течение двенадцати часов с момента выявления факта нанесения ущерба организует проведение инвентаризации имущества и подтверждение размера ущерба соответствующими документами бухгалтерского учета с расчетом его стоимости;

- обеспечивает сохранность пострадавшего имущества в том виде, в каком оно находилось после нанесения ущерба.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОРЯДКА

6.1. Контроль выполнения требований настоящего Порядка возлагается на заведующего, являющихся пользователями информационной системы персональных данных ДОУ.

6.2. Работник, нарушивший требования данного Порядка, может быть привлечен к дисциплинарной или правовой ответственности в соответствии с законодательством РФ и трудовым договором, если проступок не содержит состава преступления.