ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ГОРОДА МОСКВЫ
«ЖИЛИЩНИК РАЙОНА КОНЬКОВО»
(ГБУ «Жилищник района Коньково»)

улица Миклухо-Маклая, дом 38, г. Москва, 117279
Телефон/факс (495) 429-75-59, E-mail: gbukonkovo@uzao.mos.ru
ОГРН 5147746445688 ИНН 7728898752 КПП 772801001

ПРИКАЗ

«21» ноября 2025 г. **№ 313 - ОД**

«Об утверждении Частной Политики ГБУ «Жилищник района Коньково в отношении предоставления доступа к информационным системам и ресурсам и управления таким доступом»

В целях обеспечения выполнения мер, направленных на установление требований к предоставлению доступа к информационным системам и ресурсам и управлению таким доступом в ГБУ «Жилищник района Коньково» функций и полномочий:

1. Утвердить Частную Политику предоставления доступа к информационным системам и ресурсам и управления таким доступом в ГБУ «Жилищник района Коньково» города Москвы (далее – Политика), согласно приложению к настоящему распоряжению.
2. **Начальнику отделу персонала Прокопчук Н.В.** обеспечить доведение Политики до сведения начальников отделов, в части касающейся.
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор **О.Ю. Бяхов**

Приложение
к приказу
от «21» ноября 2025 г.
№ 313-РП

Частная Политика
предоставления доступа к информационным системам и ресурсам и управления таким доступом

1. Общие положения

Настоящая Частная Политика предоставления доступа к информационным системам и ресурсам и управления таким доступом (далее – Политика) устанавливает общие правила и требования по предоставлению и управлению доступом к информационным системам и ресурсам города Москвы, пользователями которых являются работники ГБУ «Жилищник района Коньково» города Москвы (далее - ГБУ).

2. Термины и определения

Документация по ЗИ – документы, определяющие правила и процедуры, реализуемые для обеспечения защиты информации в ИС в ходе ее эксплуатации.

Идентификатор (имя учетной записи) – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа к ИС.

ИС – информационные системы и ресурсы города Москвы, пользователями которых являются работники Префектуры.

Компрометация учетной записи – нарушение безопасности, которое приводит к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к атрибутам доступа учетной записи. Также если в рамках мониторинга событий информационной безопасности и дальнейшего его расследования были выявлены факты незаконного использования учетной записи.

Объект доступа – единица информационного ресурса, компонента ИС (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Пользователь – лицо, которому разрешено выполнять действия (операции) по обработке информации в ИС и (или) использующее результаты ее функционирования и которому в ИС присвоена учетная запись.

Ответственный за управление доступом – лицо, назначенное ответственным за управление доступом и информационную безопасность в ГБУ.

Привилегированная учетная запись – учетная запись пользователя в соответствии с установленной ролью, имеющая полномочия по

выполнению операций, касающихся функциональных возможностей по управлению (администрированию) ИС и (или) управлению (администрированию) системой защиты ИС, в том числе функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и т.д.

Публичные пользователи – лица, обращающиеся с запросом о предоставлении государственной или муниципальной услуги/функции/сервиса посредством и (или) с использованием ИС и которым в ИС присвоены учетные записи.

Работник сервисной организации – работник сервисной организации, или лица, привлекаемого сервисной организацией в качестве субподрядчика (соисполнителя) по контракту (договору) на создание, развитие (модернизацию), эксплуатацию, поддержание функционирования, сопровождение ИС и иные работы, услуги, требующие доступ к ИС.

Сервисная организация – контрагент государственного заказчика (заказчика) по контракту (договору) на создание, развитие (модернизацию), эксплуатацию, поддержание функционирования, сопровождение ИС и иные работы, услуги, требующие доступ к ИС, в том числе лица, привлекаемые контрагентом в качестве субподрядчика (соисполнителя) по контракту (договору).

Системная (технологическая) учетная запись – учетная запись, используемая для осуществления доступа к ИС программными сервисами (службами, процессами).

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Участники информационного взаимодействия – органы исполнительной власти города Москвы, подведомственные им учреждения, иные организации, определенные правовым актом Правительства Москвы, содержащим положения об ИС, должностным лицам которых в ИС присвоены учетные записи.

Учетная запись – совокупность идентификатора, пароля, прав доступа и привилегий в ИС.

Учетная запись суперпользователя (root, Administrator) – учетная запись, имеющая права и привилегии на выполнение всех без исключения операций и функций в ИС и (или) ее компонентах.

3. Общие требования к управлению доступом

3.2. Политика не регулирует вопросы доступа к информации, обрабатываемой в ИС, не требующего наличия у пользователя учетной записи.

3.3. В случае размещения компонентов ИС в инфраструктуре центра обработки данных, положения документации по ЗИ и Регламента должны учитывать установленные правила, требования, ответственность, полномочия

и порядок предоставления доступа к инфраструктуре центра обработки данных.

3.4. Если иное не установлено нормативными правовыми актами города Москвы, Ответственный за управление доступом принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие (далее – принимает необходимые меры) для разработки, утверждения и(или) доведения до сведения участников информационного взаимодействия Регламента и Политики наряду с документами по ЗИ, в части касающейся участников информационного взаимодействия.

3.5. Выполнение требований Регламента, документации по ЗИ в отношении автоматизированных рабочих мест, коммуникационного оборудования, иного программно-аппаратного обеспечения, используемого участниками информационного взаимодействия для взаимодействия с ИС обеспечивается участниками информационного взаимодействия, если иное не установлено правовым актом Правительства Москвы.

4. Общие требования к созданию учетных записей

4.1. Для каждого лица, которому предоставлен доступ к ИС, должна создаваться уникальная учетная запись пользователя. Все действия, совершаемые с использованием учетной записи пользователя, рассматриваются как совершаемые лично пользователем.

4.2. Учетные записи пользователей ИС должны быть уникальны и персонализированы (сопоставимы с реальными лицами), то есть однозначно идентифицировать своего владельца (пользователя). При наличии технической возможности создание учетных записей должно производиться с применением технологий сквозной аутентификации и (или) автоматизированной информационной системы «Система управления доступом к информационным системам и ресурсам города Москвы» в соответствии с постановлением Правительства Москвы от 02.12.2014 № 718-ПП «Об автоматизированной информационной системе «Система управления доступом к информационным системам и ресурсам города Москвы».

4.3. Исключения должны отражаться в документации по ЗИ с указанием причины.

4.4. Учетные записи суперпользователя (root, Administrator), а также системные (технологические) учетные записи должны быть закреплены за конкретными работниками.

4.5. Пользователям запрещается работать под учетными записями суперпользователей, при выполнении функций, не требующих соответствующих привилегий. При этом количество таких функций должно быть минимальным.

4.6. Пользователям запрещается работать под системными (технологическими) учетными записями. Перечень функций, выполняемых под системными (технологическими) учетными записями определяется в порядке, установленном документацией по ЗИ. За конкретными

работниками также должны быть закреплены функции по сопровождению системных (технологических) учетных записей, в том числе по выполнению таких мероприятий как:

- актуализация данных системной (технологической) учетной записи, в том числе о выполняемых ею функциях;
- соблюдение требований защиты информации в отношении системной (технологической) учетной записи;
- контроль за процессами управления доступом к системной (технологической) учетной записи;
- участие в процессах выявления и реагирование на инциденты информационной безопасности, связанные с действиями, совершаемыми с использованием системной (технологической) учетной записи.

4.7. Пользователям запрещается работать с правами привилегированных учетных записей при выполнении функций, не требующих соответствующих привилегий.

4.8.Правила разграничения доступа должны реализовываться на основе установленных списков доступа или матриц доступа и фиксироваться в документации по ЗИ.

4.9. Ответственный за управление доступом принимает необходимые меры для выполнения требований данного раздела Политики.

5. Общие требования предоставления, изменения, блокирования прав доступа

5.1. Права доступа к ИС должны предоставляться субъектам доступа в объеме, необходимом и достаточном для выполнения ими своих должностных или договорных (контрактных) обязанностей.

5.2. При увольнении из органа, учреждения или организации, а также при переводе, влекущем изменение работодателя, расторжение трудового договора/служебного контракта (далее – перевод), права доступа пользователя должны аннулироваться. Для выполнения должностных обязанностей в новом органе или организации необходимые права доступа должны запрашиваться заново.

5.3. Блокировка прав доступа пользователя должна производиться как минимум в следующих случаях:

- при увольнении/переводе или длительном отпуске (более 45 дней) пользователя;
- на основании заявки непосредственного руководителя пользователя, руководителя органа или организации;
- при расследовании или предупреждении инцидента информационной безопасности;
- при компрометации учетной записи пользователя.

5.4. При увольнении/переводе/длительном отпуске работника должна обеспечиваться блокировка всех учетных записей, которые были присвоены работнику, учетные записи, закрепленные за пользователем в соответствии с пунктами 4.4, 4.6 Политики, подлежат передаче новому ответственному лицу

с принудительной сменой паролей либо такие учетные записи подлежат блокировке.

5.5. При невозможности блокировки учетной записи производится принудительная смена паролей в отношении таких учетных записей.

5.6. Если иное не установлено нормативными правовыми актами города Москвы порядок предоставления/изменения прав доступа публичных пользователей, определяется Регламентом с учетом Политики.

5.7. Если иное не установлено правовыми актами города Москвы порядок предоставления/изменения прав доступа лиц, являющихся работниками участников информационного взаимодействия, определяется Регламентом с учетом Политики.

5.8. Запрещена работа в ИС с устройств, не обеспеченных необходимыми средствами и мерами защиты информации в соответствии с требованиями документации по ЗИ. При этом должны быть реализованы следующие минимальные меры защиты информации:

- устройства должны быть оснащены сертифицированным средством антивирусной защиты;
- устройства должны быть оснащены сертифицированным средством криптографической защиты информации, соответствующим классу защищенности ИС;
- в случае использования устройств, оснащенных видеокамерами, микрофонами и иными периферийными устройствами, должна быть реализована защита от их несанкционированной удаленной активации.

5.9. Предоставление доступа к ИС работникам сервисных организаций должно осуществляться на основании государственного контракта или договора, в ходе исполнения которого осуществляется администрирование, управление, сопровождение или обслуживание ИС (далее – контракт).

5.10. Доступ работникам сервисных организаций к ИС должен предоставляться на срок, ограниченный сроком действия контракта.

5.11. Доступ работникам сервисных организаций к ИС не должен предоставляться до реализации сервисной организацией соответствующих мер защиты и средств контроля и управления, предусмотренных документацией по ЗИ.

5.12. При заключении контракта до работников сервисной организации должно быть обеспечено доведение Регламента, а также документации по ЗИ, в части касающейся.

5.13. Порядок сопровождения учетных записей работников сервисных организаций определяется в документации по ЗИ с учетом требований Политики.

5.14. Ответственный за управление доступом организует принятие необходимых мер для выполнения требований данного раздела Политики.

6. Общие требования к контролю

6.1. Ответственный за управление доступом принимает необходимые меры для:

- контроля действий, совершаемых с использованием учетной записи пользователя в ИС;

- выявления и реагирование на инциденты информационной безопасности, связанные с действиями, совершаемых с использованием учетной записи пользователя в ИС;

- выявления неактуальных (неиспользуемых) учетных записей (в том числе сервисных и групповых), учетных записей уволенных сотрудников, а также учетных записей с избыточными правами.

6.2. Контроль и учет действий пользователей в рамках автоматизированных рабочих мест, коммуникационного оборудования, иного программно-аппаратного обеспечения, используемого для взаимодействия с ИС обеспечивается участниками информационного взаимодействия в пределах своих территориальных подразделений.

7. Ответственность

7.1. Пользователи ИС обеспечивают сохранность своих учетных данных и предпринимают необходимые действия для предотвращения их несанкционированного использования.

7.2. Пользователи ИС несут персональную ответственность за все действия, совершенные с использованием их учетной записи, за исключением случаев компрометации учетной записи не по вине пользователей.

7.3. Ответственный за управление доступом несет ответственность за принятие необходимых мер для выполнения требований Политики.