Акционерное общество «Северсталь Менеджмент»

ПРИКАЗ

10 . 07 . 2026 г. № П-ОД-700-00-26-18

г. Москва

О утверждении Положения
по управлению доступом к информационным
ресурсам группы компании «Северсталь»

В целях повышения эффективности процесса защиты от несанкционированного доступа к информационным ресурсам

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с момента подписания настоящего приказа Положение по управлению доступом к информационным ресурсам группы компаний «Северсталь» (далее - Положение) (приложение).

2. С момента подписания настоящего приказа считать утратившим силу Положение, утвержденное приказом генерального директора от 23.10.2023 г. № П-ОД-700-00-23-37.

3. Руководителям структурных подразделений АО «Северсталь Менеджмент», включая филиалы, обособленные подразделения и управляемые общества:

3.1 Организовать контроль ознакомления работников с Положением в течение 60 рабочих дней с момента подписания настоящего приказа.

3.2 Привести в соответствие с требованиями Положения локальные нормативные акты общества, содержащие требования по управлению доступом к информационным ресурсам группы компаний «Северсталь» до 30.12.2026 г.

4. Руководителям обществ, не находящихся под управлением АО «Северсталь Менеджмент», и использующих информационные ресурсы корпоративной информационной системы группы компаний «Северсталь», своими приказами распространить действие Положения на общества в течении 90 рабочих дней с момента подписания настоящего приказа.

5. Контроль исполнения приказа возложить на заместителя директора по информационной безопасности – начальника управления Гусева С. Б.

Генеральный директор А.А. Шевелев

Приложение
к приказу генерального директора
АО «Северсталь Менеджмент»
от 10.07.2026 г. № П-ОД-700-00-26-18

Положение
по управлению доступом к информационным ресурсам группы компаний «Северсталь»

г. Москва

2026 г.

СОДЕРЖАНИЕ

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Наименование документа:	*Положение по управлению доступом к информационным ресурсам группы компаний «Северсталь»*
Номер документа:	
Версия	*4*
Утверждено	*Приказом Генерального директора АО «Северсталь Менеджмент» № П-ОД-700-00-26-18 от 10.07.2026 г.*
Дата введения в действие	*«10» июля 2026 г.*
Дата пересмотра	*«10» июля 2031 г.*
Подразделение - разработчик	Управление информационной безопасности

1. НАЗНАЧЕНИЕ ДОКУМЕНТА

1.1 Настоящий документ устанавливает общие условия и требования по организации доступа пользователей к информационным системам, сервисам и ресурсам группы компаний «Северсталь» для обеспечения их информационной безопасности, а также для повышения оперативности, прозрачности и контроля управления правами доступа.

1.2 Целью настоящего документа является формирование эффективной системы управления доступом, обеспечивающей защиту информационных активов организации и предотвращение несанкционированного доступа с помощью применения ключевых принципов:

- применение минимальных привилегий (предоставление пользователям только тех прав доступа, которые необходимы для выполнения ими должностных и функциональных обязанностей);
- разделения обязанностей (SoD);
- контроля над созданием, изменением и блокировкой учетных записей;
- управления правами доступа на основе ролевой модели через единую автоматизированную систему (IDM-система);
- постоянного мониторинга текущих прав доступа пользователей и регулярного пересмотра их полномочий.

1.3 Область применения настоящего документа устанавливается для информационных систем, сервисов и ресурсов, используемых АО «Северсталь Менеджмент», и принадлежащих и используемых управляемым им обществам и их дочерним компаниям, а также иным обществам, относящимся к группе компаний «Северсталь» (далее все совместно – Общества).Требования настоящего документа распространяются на физические и (или) юридические лица, которые используют информационные системы, сервисы и ресурсы из п.1.3, в том числе в рамках договорных отношений с Обществами.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1 Политика АО «Северсталь Менеджмент» «в области защиты информации, утверждена приказом генерального директора АО «Северсталь Менеджмент» № ОРД/СМ/П-15-0000224 от 24.06.2015.

2.2 Политика АО Северсталь Менеджмент управления данными, утверждена приказом генерального директора АО «Северсталь Менеджмент» № П-ОД-700-00-26-5 от 05.03.2026.

2.3 Стандарт группы компаний Северсталь «Информационная безопасность».

2.4 ГОСТ Р 71753-2024 Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования.

3. ОСНОВНЫЕ СОКРАЩЕНИЯ

Принятое сокращение	**Полное наименование**
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
КИС	Корпоративная информационная система
КСПД	Корпоративная сеть передачи данных
КТ	Коммерческая тайна
ПДн	Персональные данные
ТСПД	Технологическая сеть передачи данных
УИБ	Управление информационной безопасности АО «Северсталь Менеджмент»
УЗ	Учётная запись
IDM	Identity Management (управление идентификационными данными)
MFA	Multi-Factor Authentication (многофакторная аутентификация)
OTP	One Time Password (одноразовый пароль)
PKI	Public key infrastructure (инфраструктура открытых ключей)

4. ОСНОВНЫЕ ТЕРМИНЫ

Аутентификация	Процедура проверки подлинности (например, проверка подлинности пользователя путем сравнения введенного пароля с сохраненным в базе данных пользовательских учетных записей).
Владелец ресурса	Работник Общества, обладающий полномочиями по определению развития, целесообразности использования информационного ресурса и правил доступа к нему, согласующий доступ на соответсвующем этапе. Каждому ресурсу назначается только один владелец.
Владелец роли	Работник Общества, ответственный за создание, изменение, удаление, назначение полномочий (в т.ч согласование заявок на доступ) и контроль доступа пользователей к инфромационным ресурсам в соответствии с их должностными обязанностями.
Внешний пользователь	Физическое лицо, работник юридического лица, не входящего в состав ГК «Северсталь», получающего доступ к КИС на основании заключенного договора оказания услуг.
Групповая учетная запись	Учетная запись для входа (работы) на компьютере несколькими работниками предприятия в случае, если невозможно организовать работу с персональными учетными записями пользователей. Например, работа в приложениях, которые не дают возможности многопользовательской аутентификации или на компьютерах в учебных классах, тестирования персонала.
Домен	Служба каталогов иерархической структуры, в которой хранятся сведения об объектах (учетные записи пользователей, пароли, компьютеры, принтеры, общие ресурсы и т.д.) и которая позволяет пользователям в той же сети получать доступ к этой информации.
Доступ	Возможность использования информационных ресурсов.
Информация	Сведения (сообщения, данные) независимо от формы их представления.

Информация, подлежащая защите (защищаемая информация)	Информация, составляющая коммерческую тайну, определенная Перечнем информации, составляющей коммерческую тайну Общества, персональные данные, определенные Перечнем персональных данных, обрабатываемых в Обществе, иная охраняемая законом информация и сведения ограниченного доступа.
Информационный ресурс	Предметно-ориентированный элемент информационной системы, использующийся в модели разграничения доступа информационной системы как объект доступа.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Корпоративная информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, используемых на предприятиях группы компаний «Северсталь».
Корпоративная сеть передачи данных	Телекоммуникационная сеть, объединяющая в единое информационное пространство все структурные подразделения компании и обеспечивающая одновременную передачу данных, взаимодействие приложений, расположенных в различных узлах, доступ к ним пользователей.
Корпоративное ИТ-подразделение	ИТ-подразделение, в обязанности которых входит обработка обращений пользователей по восстановлению ИТ-сервисов и оказание консультаций по вопросам, касающимся использования КИС Общества, обеспечение предоставления ИТ-сервисов.
Корпоративный пользователь	Физическое лицо, имеющее доступ к ресурсам корпоративной информационной системы Общества посредством вычислительной техники и действующий трудовой договор с юридическим лицом ГК Северсталь
Корпоративное оборудование	Стационарный компьютер, ноутбук, планшет, промышленный мобильный терминал и т.п. или иное устройство, на которое распространяются политики и настройки КИС
Несовместимые полномочия	Уровень полномочий на использование информационного ресурса, превышающий основные обязанности работника Общества.

Ответственное лицо	Работник Общества, имеющий корпоративную учетную запись и попадающий хотя бы под одну из следующих категорий: - линейный руководитель пользователя; - функциональный руководитель; - руководитель проекта в интересах которого пользователю создается УЗ или предоставляется доступ к ИР; - согласующий доступ пользователю к ИР на этапе «Руководитель», назначенный в системе согласования доступа.
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Подменный фонд	Устройства, предназначенные для временного использования на период выезда за пределы территории РФ (за соответствующим исключением).
Привилегированный доступ	Доступ к ресурсам (системам, данным) с расширенными правами, позволяющий выполнять действия, влияющие на работу и целостность инфраструктуры, включая изменение настроек, управление конфигурациями и выполнение операций с высоким уровнем риска для безопасности и работоспособности инфраструктуры организации.
Роль	Набор полномочий, предоставленных пользователю для осуществления конкретных действий в информационной системе (создание записей, редактирование данных, просмотр отчетов и др.), позволяющих ограничить доступ пользователей только теми функциями и информацией, которые необходимы для выполнения должностных обязанностей.
Ролевая модель	Формализованный и заранее определённый набор ролей в информационных системах, ресурсам, соответствующий функциональным обязанностям пользователя
Средства аутентификации	Пароль, пин-код и иной код для проверки подлинности учетной записи пользователя.

Телефонный номер для SMS информирования	Номер мобильного телефона пользователя, используемый для уведомлений о событиях с его учетной записью (истечение срока действия пароля, смена пароля и др.), зарегистрированный в «Личном кабинете SAP» и/или на корпоративном портале в сервисе «Мои контакты», либо указанный пользователем при оформлении заявки на создание учетной записи.
Технологическая сеть передачи данных	Телекоммуникационная сеть, объединяющая в единое информационное пространство элементы АСУП и ТП и обеспечивающая одновременную передачу данных, взаимодействие приложений, расположенных в различных узлах, доступ к ним пользователей.
IDM -система	Информационная система централизованного управления учетными записями и правами доступа пользователей в корпоративных информационных системах.
MFA	Метод контроля доступа, при котором пользователю нужно подтвердить свою личность с помощью двух или более независимых факторов (многофакторная аутентификация).
OTP	Одноразовый пароль, который действителен только для одного сеанса аутентификации.

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Под управлением доступом понимается процесс управления всем жизненным циклом прав доступа к информационным ресурсам, включающий:

а). предоставление учетных записей с минимально необходимыми полномочиями на основании функциональных обязанностей;

б). регулярный пересмотр полномочий в целях актуализации доступа;

в). изменение прав доступа в связи с изменением функциональных обязанностей пользователей или требований информационной безопасности;

г). блокировку прав доступа пользователя в случае обнаружения угроз, инцидентов информационной безопасности;

д). отзыв доступа при увольнении, завершении контракта или по другим причинам.

Управление доступом должно осуществляться в соответствии с требованиями информационной безопасности, внутренними нормативными документами и действующим законодательством.

5.2 Доступ осуществляется посредством ролевых моделей, являющихся основным инструментом управления полномочиями пользователей в информационных системах, сервисах и ресурсах Общества. Дополнительный доступ предоставляется на основании информации в согласованной в установленном порядке заявке, поданной в электронном виде с помощью портала самообслуживания (Каталог ИТ-услуг, SAP GRC).

5.3 Для каждой ролевой модели (матрицы) доступов и роли доступа должен быть определён бизнес-владелец, ответственный за её актуальность, эффективность и соответствие бизнес-задачам.

5.4 Ролевые модели (матрицы) доступа и роли доступа должны быть разработаны таким образом, чтобы исключать или минимизировать несовместимые права доступа (SoD-конфликты).

5.5 Требования к управлению доступом применяются ко всем информационным системам, сервисам и ресурсам Общества независимо от их назначения или среды эксплуатации (разработка, тестирование, продуктив):

5.5.1 Для систем разработки:

а). допускается отклонение от строгого следования ролевой модели;

б). допускается предоставление доступа с профилями типа "полный доступ";

в). доступ конечных пользователей ограничивается по функционалу и сроку действия.

5.5.2 Для систем тестирования:

а). применение ролевой модели является обязательным;

б). запрещен доступ с профилями "полный доступ", кроме работников корпоративного ИТ-подразделения, выполняющих функции системного администрирования;

в). работникам корпоративного ИТ-подразделения, выполняющим функции поддержки, предоставляется доступ с правами на внесение изменений.

5.5.3 Для продуктивных систем:

а). применение ролевой модели является обязательным;

б). запрещен доступ с профилями "полный доступ" (кроме работников корпоративного ИТ-подразделения, выполняющих функции системного администрирования);

в). внешние пользователи могут иметь права доступа, если это предполагает бизнес-процесс;

г). работникам корпоративного ИТ-подразделения, выполняющим функции поддержки, предоставляется по умолчанию доступ только на просмотр, в отдельных случаях с ограниченными правами на внесение изменений, а расширенные полномочия предоставляются по отдельному запросу.

5.6 IDM-система является источником данных об учетных записях, ролевых моделях и правах доступа и используется для централизованного администрирования.

5.7 Все вводимые в эксплуатацию информационные системы должны быть интегрированы с IDM-системой или иметь возможность подобной интеграции. Управление доступом в обход IDM-системы возможно только в случаях технической невозможности реализации интеграции, а также в случаях отдельного согласования с УИБ.

5.8 Корпоративное ИТ-подразделение осуществляет:

а). сопровождение справочника контрагентов;

б). классификацию предприятий (корпоративное/внешнее);

6. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И РОЛЯМИ

6.1 К ресурсам относятся все компоненты информационных систем, доступ к которым регулируется. К таким ресурсам относятся базы данных, папки с файлами, отдельные файлы, приложения и другие элементы, к которым может быть предоставлен доступ.

6.2 Каждый ресурс должен обладать набором атрибутов, таких как, наименование, описание, конфиденциальность, тип ресурса, категория ресурса, местоположение, бизнес-единица, период действия, процедура согласования, владелец и др. На протяжении жизненного цикла ресурса состав атрибутов может изменяться.

6.3 Ресурс может быть добавлен в Каталог ИТ-услуг в рамках:

а). публикации нового сервиса/услуги;

б). заявки на создание нового объекта сервиса/услуги, который учитывается как информационный ресурс в Каталоге ИТ-услуг (новая общая папка, новый групповой ящик и т.д.);

в). аудита по сервису/услуге;

г). изменения структуры Каталога ИТ-услуг (слияние/разделение сервисов).

6.4 Ресурс может быть закрыт в Каталоге ИТ-услуг в рамках:

а). заявки на удаление/блокирования объекта сервиса/услуги;

б). вывода сервиса/услуги из эксплуатации;

в). аудита по сервису/услуге при фактическом отсутствии/неактуальности ресурса;

г). изменения структуры Каталога ИТ-услуг (слияние/разделение сервисов);

д). решение владельца ресурса.

6.5 Назначение владельцев ресурсов в каталоге ИТ-услуг и (или) ролей в SAP GRC осуществляется руководителем подразделения или уполномоченным лицом Общества. Работник, назначаемый владельцем ресурса и (или) роли, должен обладать достаточным уровнем компетенции и полномочий для принятия решений о предоставлении доступа с учетом приниципа минимизации полномочий и обеспечения безопасности ресурсов.

6.6 Владелец ресурса в каталоге ИТ-услуг совместно с работниками ИБ и ИТ подразделений определяют маршрут согласования запросов на доступ. Маршрут может быть пересмотрен на основании заявки.

6.7 В маршруты согласования заявок на доступ к ресурсам в каталоге ИТ-услуг и (или) ролям в SAP GRC для внешних пользователей в обязательном порядке включается этап согласования «Руководитель», в роли которого выступает Ответственное лицо.

6.8 Владелец ресурсов в каталоге ИТ-услуг и (или) ролей в SAP GRC может определить заместителя, который:

а). получает все полномочия владельца на управление доступом;

б). назначается на постоянный или временный период (отпуск, болезнь и т.д.).

6.9 Владелец ресурса в каталоге ИТ-услуг определяет категорию защищаемой информации (КТ, ПДн), которую можно обрабатывать (хранить, передавать) при использовании ресурса и обеспечивает фиксацию результатов своей оценки на соответствующем портале самобслуживания (Каталог ИТ-услуг).

7. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ

7.1 В зависимости от используемых информационных систем и способов аутентификации пользователям создаются соответствующие учетные записи (персональные, групповые):

а). для работы с ИС, при аутентификации в которых используются учетные записи домена КСПД, пользователю создается уникальная персональная учетная запись в соответствующем домене КСПД;

б). для работы с ИС, при аутентификации в которых используются учетные записи домена ТСПД, пользователю может быть создана дополнительная учетная

запись в соответствующем домене ТСПД;

в). для работы с ИС, в которых возможна только аутентификация с помощью локальной УЗ, пользователю может быть создана дополнительная учетная запись на уровне ИС.

7.2 Для персональных учетных записей установлены следующие требования:

а). должны быть уникальными для однозначной идентификации пользователя и не повторять свойства архивных учетных записей;

б). наименование (логин) формируется с использованием латинских букв и цифр;

в). транслитерация кириллицы выполняется по стандарту ИКАО Doc 9303 (Раздел IV, часть 1).

7.3 Перед созданием персональной учетной записи пользователь должен быть ознакомлен с нормативными актами в области ИТ и ИБ.

7.4 Факт ознакомления с нормативными актами в области ИТ и ИБ фиксируется:

а). в бумажном виде в листе регистрации ознакомления/ ответственности пользователя (Приложение 1);

б). в электронном виде в отдельной форме специализированной информационной системы.

7.5 Оригинал листа регистрации ознакомления/ответственности работника хранится в кадровой службе Общества:

7.6 Учетная запись для работников Общества (по трудовому договору или договору ГПХ) создается по проставленному коду мероприятия в кадровой системе (SAP HCM) или по заявке кадровой службы предприятия, учет персонала которого ведется в иных системах.

7.7 Учетная запись для внешних пользователей создается по заявке от любого пользователя – работника Общества. При оформлении заявки инициатор должен приложить скан-копии документов (Приложение 2). В маршрут согласования заявки обязательно включается Ответственное лицо и работник ИБ.

7.8 Учетная запись должна иметь ограничение по сроку использования:

а). для работников Общества срок определяется датой действия трудового договора или договора ГПХ, отражается в кадровой системе (SAP HCM) и в иных системах, в которых ведется учет персонала;

б). для внешних пользователей срок определяется на период в один год (365 дней), если иной срок не указан в документе, обосновывающим создание учетной записи.

7.9 Для групповой учетной записи:

а). должен быть определен владелец;

б). назначение владельца согласуется непосредственным руководителем;

в). любые изменения учетной записи должны согласовываться с владельцем;

г). не допускается использование для доступа к ресурсам с защищаемой информацией, за исключением необходимости обеспечения непрерывности технологических процессов при соблюдении мер контроля и мониторинга.

7.10 При использовании групповых учетных записей Корпоративное ИТ-подразделение обеспечивает:

а). учет и периодическую инвентаризацию владельцев (не реже 1 раза в 6 месяцев);

б). наличие информации обо всех имеющих к ней доступ пользователей;

в). запуск процедуры смены пароля при блокировке (п. 7.14 «а»-«б», «г», «ж»-«л») персональной учетной записи владельца и (или) персональной учетной записи эксплуатирующего ее пользователя;

г). учет оборудования/информационных ресурсов, на которых она используется.

7.11 При создании учетной записи устанавливается первичный пароль, который пользователь обязан сменить при первом входе в ИС.

7.12 Для передачи первичного пароля используются следующие каналы передачи:

а). телефонный номер для SMS информирования;

б). корпоративная электронная почта ответственного лица, указанного в заявке (некорректный или отсутствующий телефонный номер, либо SMS-сообщение не доставлено адресату).

При невозможности использования технических каналов передача пароля осуществляется на бумажном носителе в запечатанном конверте.

7.13 По запросу работника УИБ может быть инициирована принудительная смена пароля от учетной записи пользователя.

7.14 Учётная запись блокируется в течение 1 календарного дня при наступлении событий:

а). истечение срока действия учётной записи;

б). увольнение без последующего приёма внутри ГК «Северсталь»;

в). перевод на лёгкий труд, отпуск по беременности/уходу за ребёнком;

г). приостановление трудового договора при мобилизации;

д). увольнение с последующим приёмом внутри ГК «Северсталь»;

е). отстранение от работы (кроме доступа к личному кабинету SAP HCM);

ж). требование работника УИБ;

з). уведомление об увольнении работника подрядной организации, либо расторжении договора с подрядной организацией. Ответственное лицо передает эту информацию сотрудникам корпоративного ИТ-подразделения;

и). мотивированное требование ответственного лица;

к). неиспользование в течение 180 календарных дней или превышение на 60 дней срока смены пароля с истекшим периодом действия;

л). непрохождение обязательного обучения (для работников компании: «Первичный инструктаж по ИБ», для контрагентов – «Базовый курс по ИБ для контрагентов»).

7.15 Для сохранения полномочий учетной записи при событиях п. 7.14, «б», «в», «г» и в особом случае – «а», ответственным лицом создается запрос на сохранение полномочий. Срок сохранения полномочий по событию «б» - не более 30 календарных дней.

7.16 При наступлении событий пункта 7.14 «д» полномочия учетной записи могут быть переназначены на новую учетную запись работника по новому месту работы:

а). переназначенные полномочия должны быть подтверждены участниками согласования в течение 14 календарных дней;

б). неподтвержденные полномочия отзываются автоматически.

7.17 При наступлении событий пункта 7.14 «е», «ж», «и», «л» учетная запись разблокируется только при устранении условий возникновения блокировки.

7.18 При переводе внутри юридического лица в отношении учетной записи работника:

а). Действующий руководитель в течении 5 рабочих дней принимает решение о сохранении или блокировке ранее предоставленных дополнительных доступов, при этом доступы по ранее предоставленной ролевой модели автоматически отзываются;

б). при необходимости использования на новом рабочем месте заблокированных полномочий создается заявка.

7.19 При переходах работников в другое юридическое лицо ГК «Северсталь» с сохранением функциональных обязанностей:

а). кадровой службой проставляется код мероприятия в кадровой учетной системе (SAP HCM) или создаётся заявка на перевод;

б). учётная запись не блокируется;

в). существующие полномочия учетной записи не отзываются.

7.20 Заблокированная учетная запись пользователя при увольнении или по окончанию срока действия договора должна быть удалена через 14 календарных дней.

7.21 Корпоративное ИТ-подразделение обязано сохранять в течение 3 лет информацию об удаленной учетной записи (уникальные идентификаторы, в т. ч. дату и время удаления).

8. ПРЕДОСТАВЛЕНИЕ, ИЗМЕНЕНИЕ И ПРЕКРАЩЕНИЕ ДОСТУПА

8.1 Доступ осуществляется с помощью ИТ-сервисов, предоставление которых зависит от

а). категории пользователя (корпоративный/внешний);

б). параметров, указанных в сервисном договоре Общества, юридического и (или) физического лица, работающего по гражданско-правовому договору, с внутренним провайдером ИТ-услуг.

8.2 Корпоративное ИТ-подразделение в установленные сроки реализует технические мероприятия для предоставления доступа к ресурсам каталога ИТ-услуг и ролям SAP GRC на основании заявок.

8.3 Предоставление доступа осуществляется одним из способов согласно приоритету:

а). через IDM-систему — добавление атрибутов к учётной записи в целевой ИС;

б). через специализированный модуль ИС (например, SAP GRC) – присвоение ролей и полномочий;

в). через систему идентификации и управления доступом Keycloak;

г). напрямую администратором ИС.

8.4 Первичный доступ новому пользователю-работнику предприятия предоставляется автоматически на основании:

а). зафиксированной в IDM-системе ролевой модели (матрицы) для его должности;

б). данных из кадровой системы;

в). данных из иной системы, в которой ведется учет персонала

8.5 Работникам корпоративного ИТ – подразделения может быть предоставлен привилегированный доступ (присвоены полномочия, создана учетная запись) для работы с информационными системами, только с соблюдением следующих мер:

а). использование выделенных административных рабочих мест (Privileged Access Workstation, PAW) для доступа к инфраструктурным системам;

б). построение многоуровневой модели администрирования (Tier Administrative Model) для инфраструктурных систем;

в). реализация процесса управления и контроля использования временного повышенного (экстренного) доступа (полномочия Fire Fighter для SAP-систем).

8.6 В процессе обработки заявки на доступ на этапе «Руководитель», Ответственное лицо:

а). проверяет корректность заполнения заявки;

б). определяет необходимость предоставления запрошенных прав доступа, руководствуясь функциональными обязанностями пользователя;

в). оценивает потенциальные риски от наличия у пользователя несовместимых полномочий;

г). согласовывает заявку на своём этапе при отсутствии противоречий.

8.7 В процессе обработки заявки на доступ на этапе «Владелец», Владелец ресурса Каталога ИТ-услуг и (или) роли SAP GRC:

а). определяет возможность предоставления запрошенных прав доступа с учетом принципа минимизации полномочий;

б). осуществляет оценку соответствия запрошенного доступа поставленным заявителю задачам.

8.8 В процессе обработки заявки на доступ к ресурсу работник УИБ в течении двух рабочих дней:

а). проверяет наличие подписанного соглашения о конфиденциальности;

б). проверяет наличие подписанного соглашения об обеспечении информационной безопасности (при необходимости его заключения);

в). оценивает отсутствие противоречий с внутренними нормативными документами;

г). оценивает наличие иной информации, препятствующей получение доступа к ресурсу Каталога ИТ-услуг и (или) роли SAP GRC.

8.9 В случаях выявления замечаний или несоответствий заявка на доступ отклоняется с указанием причин.

8.10 При необходимости получения дополнительной информации от инициатора срок обработки запроса увеличивается пропорционально времени получения ответа. При отсутствии ответа в течении 5 рабочих дней – заявка отклоняется.

8.11 Заявки на предоставление доступа к ресурсам от пользователей, относящихся к категории ТОП 30 АО «Северсталь Менеджмент», проходят процедуру обработки без этапа согласования «Руководитель».

8.12 Права доступа подлежат корректировке:

а). при изменении организационной структуры предприятия/подразделения;

б). при изменении должностных или функциональных обязанностей;

в). по результатам аудита полномочий и прав доступа.

8.13 Инициатором заявки на изменения (корректировку) прав доступа может выступить:

а). работники корпоративного ИТ-подразделения, ответственные за сопровождение системы централизованного управления учетными записями и правами доступа пользователей в корпоративных информационных системах;

б). непосредственный пользователь;

в). линейный/функциональный руководитель;

г). владелец ресурса;

д). работники смежных подразделений;

е). работники УИБ.

8.14 Изменение (корректировка) полномочий и прав доступа производится на основании действий с элементами ролевой модели:

а). создание новых ролей доступа;

б). изменение и (или) удаление существующих ролей.

8.15 Полностью доступ пользователя прекращается при достижении сроков действия учетной записи, реализуется в автоматическом режиме средствами IDM-системы:

а). для работников Общества на основе данных из кадровой системы (SAP HCM) или иной системы, в которой ведется учет персонала;

б). для внешних пользователей на основании данных о сроке действия учетной записи.

8.16 Прекращение доступа к отдельным ресурсам Каталога ИТ-услуг или ролям SAP GRC, либо полное прекращение доступа возможно также по инициативе Ответственного лица, владельца ресурса, роли или работника УИБ. Выполняется работниками корпоративного ИТ-подразделения и регистрируется в соответствующей учетной системе.

9. ОРГАНИЗАЦИЯ УДАЛЕННОГО ДОСТУПА

9.1 Удаленный доступ к ресурсам предоставляется по заявкам. Обязательным является использование MFA (сертификат PKI, код из приложения, Push-уведомления, OTP, SMS). Способы подключения определены в приложении 3.

9.2 Для пользователей, перечисленных в приложении 4, доступ организуется только с применением сертификата PKI на аппаратном ключе (токене). Временное подключение к корпоративным ресурсам с применением технологии MFA (не более 21 дня) до получения корпоративного оборудования разрешено:

а). работникам с дистанционным форматом работы – терминальный доступ (п.4 приложения 3);

б). внешним пользователям, осуществляющим разработку и поддержку информационных систем – терминальный доступ (п. 5-6 приложения 3), удаленный рабочий стол (п. 8,10 приложения 3), шлюз мониторинга (п. 9 приложения 3).

9.3 Для работников ИТ-функции, выезжающих для работы за пределы Российской Федерации:

а). в учетной системе, в которой ведется учет персонала работнику устанавливается признак «Пользователь за пределами РФ»;

б). действущая учетная запись работника блокируется и удаляется, за исключением случаев, согласованных с УИБ;

в). для работы создается новая учетная запись;

г). при согласовании дополнительных прав доступа в учетной системе согласующие информируются о том, что пользователь будет находится за пределами РФ;

д). удаленный доступ предоставляется с личных устройств или с подменного фонда. Допустимые типы удаленного доступа определены п. 2, 4, 6-10 приложения 3;

е). привилегированный доступ к системам SAP (полномочия Fire Fighter для SAP-систем) могут быть выданы на срок не более 5 рабочих дней.

9.4 Удаленный доступ не предоставляется для:

а). работников специальных подразделений;

б). работников кадровой службы, ведущих воинский учет.

9.5 Организацию любых ИТ-сервисов с применением технологии удаленного доступа, включая установку и настройку программного обеспечения, осуществляют работники Корпоративного ИТ-подразделения.

9.6 Каждый сеанс удалённого доступа должен проходить повторную аутентификацию.

9.7 Для ресурсов и информационных систем с удаленным доступом в обязательном порядке включается журнал аудита событий с фиксацией:

а). время начала и завершения сеанса удалённого подключения;

б). сетевого адреса источника и назначения;

в). типа подключения;

г). идентификатора пользователя и устройства, с которого выполнено подключение.

9.8 Все удалённые подключения должны ограничиваться средствами разграничения сетевого доступа, контролироваться средствами защиты информации.

9.9 Доступ к информационным системам, сервисам и ресурсам Обществ для работников ИТ-функции, работающих из иностранных государств, предоставляется в особом порядке, включая:

а). создание новых учетных записей;

б). авторизацию через личные устройства и санкционированные виды подключений;

в). запрет на вывоз ИТ-оборудование Общества за пределы РФ, за исключением подменного фонда.

10. КОНТРОЛЬ ПРИСВОЕННЫХ ПРАВ И ПОЛНОМОЧИЙ ДОСТУПА

10.1 Владелец ресурса каталога ИТ-услуг обязан регулярно (не менее 1 раза в 6 месяцев) проводить контроль актуальности и корректности присвоенных прав и полномочий доступа. Для этого применяется:

а). функционал портала самообслуживания (Каталог ИТ-услуг);

б). специализированное программное обеспечение, уведомляющее владельца ресурса о необходимости проведения проверки.

10.2 Контроль должен выявлять:

а). неактуальные учетные записи (уволенные работники, неиспользуемые УЗ);

б). избыточные права доступа (нарушение принципа минимальных привилегий);

в). учетные записи, не имеющие владельца;

г). накопленные права доступа, не соответствующие функциональным и должностным обязанностям работников Общества;

д). нарушение установленных процедур присвоения доступов.

10.3 Внеплановый контроль может осуществляться работниками УИБ, управления внутреннего аудита (УВА) и управления риск-менеджмента и внутреннего контроля (УРМиВК).

10.4 По результатам проведения контрольных мероприятий принимается решения об изменении учётных записей, ролевых моделей (матриц) и прав доступа (удаление, изменение сроков действия доступов), устранение избыточных прав.

11. ОТВЕТСТВЕННОСТЬ

11.1 Ответственное лицо несет ответственность за:

а). проверку обоснованности запрашиваемых прав доступа;

б). оценку рисков получения пользователем несовместимых полномочий;

в). сохранность и конфиденциальность переданного пароля для пользователя;

г). идентификацию пользователя при передаче ему пароля.

11.2 Работник ИТ-подразделения несет ответственность за:

а). сохранность и конфиденциальность созданного для пользователя первичного пароля;

б). корректность предоставления полномочий и прав доступа по заявкам пользователей;

в). реализацию технических мероприятий, необходимых для обеспечения корректной и бесперебойной работы процесса управления доступом;

г). корректность ведения и доступность справочника контрагентов;

д). сохранность информации об удаленных учетных записях;

е). учет владельцев групповой учетной записи и их периодическую инвентаризацию;

ж). наличие информации в учетной системе о пользователях, имеющих доступ к групповой УЗ;

з). запуск процедуры смены пароля от групповой учетной записи в случае увольнения владельца или работника, имеющего доступ к такой УЗ;

и). учет оборудования/ИР, на котором будет использоваться групповая УЗ.

11.3 Работник УИБ несет ответственность за:

а). проверку наличия необходимых документов, обязательных для предоставления доступа;

б). своевременность обработки запросов на этапе согласования «службы информационной безопасности»;

в). проверку отсутствия стоп-факторов для предоставления доступа;

г). соответствие настроек подсистем управления доступом требованиям информационной безопасности;

д). обеспечение контроля за соблюдением владельцами ресурса правил периодического пересмотра прав доступа пользователей.

11.4 Владелец ресурса Каталога ИТ-услуг и (или) роли SAP GRC несет ответственность за:

а). корректность и своевременность фиксации и актуализации данных о ресурсе на портале самообслуживания (Каталог ИТ-услуг, SAP GRC);

б). принятие решений по вопросам создания и ликвидации ресурса Каталога ИТ-услуг и (или) роли SAP GRC;

в). своевременность проведения актуализации прав доступа к ресурсу Каталога ИТ-услуг и (или) роли SAP GRC;

г). своевременность реагирования на уведомление о необходимости проведения контроля за актуальностью и корректностью присвоения прав доступа;

д). оценку ресурса Каталога ИТ-услуг на соответствие категории конфиденциальности;

е). оценку соответствия задачам бизнеса запрашиваемых прав доступа.

11.5 В случаях нарушения требований настоящего положения работники Общества несут ответственность в порядке, установленном законодательством.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1 Сроки и порядок вступления в силу настоящего Положения определяются приказом об его утверждении. Настоящее Положение действует без ограничения сроков.

12.2 Если в результате изменения законодательства отдельные положения настоящего нормативного документа вступают в противоречие с действующим законодательством, то указанные положения утрачивают силу.

12.3 Внесение изменений и дополнений в настоящее Положение осуществляется приказом Генерального директора Общества.

12.4 Общую ответсвенность за актуальность положения несет Управление информационной безопасности.

Приложение 1

_____

_____

(наименование организации, в которой работает пользователь)

_____

_____

(наименование подразделения)

Лист регистрации
ознакомления / ответственности пользователя

_____

(ФИО, должность)

_____

№ п/п	Наименование документа	Личная подпись[1]	Дата
1	Политика АО «Северсталь Менеджмент» в области защиты информации.		
2	Политика АО «Северсталь Менеджмент» в области обработки персональных данных.		
3	Политика парольной защиты группы компаний «Северсталь».		
4	Инструкция пользователя корпоративной информационной системы группы компаний «Северсталь».		
5	Положение по управлению доступом к информационным ресурсам группы компаний «Северсталь»[2]		

Даю своё согласие на отправку информационных SMS-сообщений на номер _____

номер телефона

_____

(подпись пользователя)

Личную подпись пользователя УДОСТОВЕРЯЮ

_____

_____ _____

(ФИО руководителя подразделения) (подпись руководителя, печать для внешних организаций)

1 Подтверждаю собственноручной подписью, что все перечисленные документы мною прочитаны и их содержимое мне понятно.

2 Ознакомление только для работников Обществ

Приложение 2

Перечень предоставляемых документов

Группа пользователей	**Предоставляемые документы**
Внешний пользователь (не работник Общества)	1. Лист регистрации ознакомления / ответственности пользователя 2. Документ, обосновывающий создание учетной записи (ссылка на договор, электронная копия протокола, распоряжение/приказ руководства Общества и т.п.) 3. Соглашение о конфиденциальности (NDA) между внешним физическим или юридическим лицом и Обществом в случае необходимости доступа к ИР содержащим информацию, составляющую коммерческую тайну Общества;

Приложение 3

Способы удаленного подключения

№ п/п	Тип удаленного доступа	Ресурсы для доступа	Вид устройства	Тип пользователя
1	Доступ к ИТ-ресурсам из Интернет с корпоративных ноутбуков или ПК (VPN-Corp)	Ресурсы, объявленные общекорпоративными	Корпоративные	Корпоративный
2	VPN-Util-<код_проекта>	Доступ к отдельно взятому ресурсу (списку ресурсов)	Корпоративные и некорпоративные	Корпоративный, некорпоративный
3	VPN-Adm-<код_проекта (процесса)>	Ресурсы, объявленные общекорпоративными. Дополнительные заявленные ресурсы	Корпоративные	Корпоративный
4	Доступ к ИТ-ресурсам из Интернет (на терминал RDSFarm-Corpusers)	Ресурсы, объявленные общекорпоративными	Корпоративные и некорпоративные	Корпоративный
5	Доступ к ИТ-ресурсам из Интернет для некорпоративных пользователей (RDSFarm-ExtUsers)	Ограниченный список корпоративных ресурсов	Некорпоративные	Некорпоративный
6	Доступ к ИТ-ресурсам из Интернет для доступа к SAP внешних разработчиков (stal-rds-dev)	Ограниченный список корпоративных ресурсов	Корпоративные и некорпоративные	Корпоративный, некорпоративный
7	Удаленный доступ к ИТ-ресурсам из Интернет с некорпоративных ноутбуков/ПК на рабочий ПК (RDP до рабочей станции (GW))	Доступ к отдельно взятому ресурсу (списку ресурсов)	Корпоративные и некорпоративные	Корпоративный

8	Удаленный доступ к ИТ-ресурсам из Интернет по RDP до windows сервера через шлюз удаленных рабочих столов (RDGW)	Специализированные ресурсы	Корпоративный, некорпоративный	Корпоративный, некорпоративный
9	Удаленный доступ к ИТ-ресурсам из Интернет через шлюз мониторинга (PAM)	Специализированные ресурсы	Корпоративные и некорпоративные	Корпоративный, некорпоративный
10	Удаленный доступ к ИТ-ресурсам из Интернет через виртуальное рабочее место (VDI)	Ресурсы, объявленные общекорпоративными. Специализированные ресурсы.	Корпоративные и некорпоративные	Корпоративный, некорпоративный

Приложение 4

Перечень категорий пользователей, для которых использование сертификата PKI на аппаратном ключе (токене) в качестве второго фактора аутентификации является обязательным

1. Руководители ТОП -12, ТОП-100.
2. Генеральные, функциональные директора, начальники управлений.
3. Секретари и (или) помощники руководителей из п.п. 1 и 2.
4. Работники бизнес-единиц: ООО «Северсталь-ЦЕС», АО «Северсталь-Инфоком», ООО «Северсталь-СКИФ», ООО «Делетрон».
5. Работники подразделений: СОБ, УРМиВК, УВА, финансовой функции.
6. Работники Общества и работники подрядчиков, занимающиеся наладкой и обслуживанием информационных систем и оборудования на объектах критической информационной инфраструктуры.
7. Работники Общества, занимающиеся сопровождением инфраструктуры АСУ ТП (сетей, контроллеров, серверов, рабочих станций).
8. Работники Общества, имеющие доступ к строго конфиденциальной информации, биометрическим и специальным категориям персональных данных.
9. Работники Общества, работающие с системами банк-клиент.
10. Внешние подрядчики, осуществляющие разработку и поддержку информационных сервисов и систем.