Приложение
УТВЕРЖДЕНО
приказом Генерального директора
АО «Северсталь Менеджмент»
№ П-ОД-700-00-23-37 от 23.10.2023 г.

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

г. Москва
2023 г.

СОДЕРЖАНИЕ

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Наименование документа:	*Положение по управлению доступом к информационным ресурсам АО «Северсталь Менеджмент»*
Номер документа:	
Версия	*3*
Утверждено	*Приказом Генерального директора АО «Северсталь Менеджмент» № П-ОД-700-00-23-37 от 23.10.2023 г.*
Дата введения в действие	*«23» октября 2023 г.*
Дата пересмотра	*30 октября 2025 г.*

1. НАЗНАЧЕНИЕ ДОКУМЕНТА

1.1 Настоящее Положение устанавливает единый порядок управления доступом к информационным ресурсам корпоративной информационной системы (далее КИС).

1.2 Целью настоящего Положения является упорядочивание предоставления, изменения прав доступа к информационным ресурсам КИС.

1.3 Требования настоящего документа распространяются на работающих с КИС работников юридических лиц группы компаний «Северсталь» (далее Обществ) и сторонних организаций при работе с информационными ресурсами Обществ.

2. НОРМАТИВНЫЕ ССЫЛКИ

Политика Общества в области защиты информации
Стандарт группы компаний Северсталь «Информационная безопасность»

3. ОСНОВНЫЕ СОКРАЩЕНИЯ

Принятое сокращение	Полное наименование
КИС	Корпоративная информационная система
ТСПД	Технологическая сеть передачи данных
КСПД	Корпоративная сеть передачи данных
ИС	Информационный сервис
ИР	Информационный ресурс
УИБ	Управление информационной безопасности
СПП	Служба поддержки пользователей
КТ	Коммерческая тайна
ПДн	Персональные данные
PKI	public key infrastructure (инфраструктура открытых ключей)

4. ОСНОВНЫЕ ТЕРМИНЫ

Аутентификация	Процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользовательских учетных записей
Владелец информационного ресурса	Работник предприятия, обладающий полномочиями по определению развития, целесообразности использования информационного ресурса и правил доступа к нему. Каждому ресурсу назначается только один владелец.
Групповая учетная запись	Обезличенная учетная запись для входа(работы) на компьютер несколькими сотрудниками предприятия в случае, если невозможно организовать работу с личными учетными записями пользователей. Например, работа в приложениях, которые не дают возможности многопользовательской аутентификации или на компьютерах в учебных классах, тестирования персонала.
Домен (Active Directory)	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.
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 (ИР)	Предметно-ориентированный объем данных, который может содержать документы, каталоги, базы данных, и доступ к которым осуществляется с помощью информационного сервиса.
Информационный сервис (ИС)	Программно-аппаратный комплекс, предоставляющий доступ и взаимодействие пользователя с различной информацией.
Изменение прав доступа к ИР	Повышение или понижение уровня полномочий на использование информационного ресурса.
Корпоративная информационная система (КИС)	Совокупность находящейся в электронном виде информации и всех обеспечивающих ее обработку информационных технологий и технических средств, используемых на предприятиях группы компаний «Северсталь».
Корпоративная сеть передачи данных (КСПД)	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.
Средства аутентификации	Пароль, пин-код и иной код для проверки подлинности учетной записи пользователя.

Технологическая сеть передачи данных ТСПД	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.
Корпоративное ИТ-подразделение	Сотрудники ИТ-подразделения, 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 устройство	Рабочая станция или иное устройство, на которое распространяются политики и настройки КИС
Мобильный компьютер	Переносное средство вычислительной техники (ноутбук, планшет, промышленный мобильный терминал и т.п.)
Несовместимые полномочия	Уровень полномочий на использование информационного ресурса, превышающий основные обязанности работника Общества, или вызывающие конфликтные полномочия.
Критичные полномочия	Полномочия, предоставляющие доступ к коммерческой тайне категории строго конфиденциально, специальным и биометрическим персональным данным, а также полномочия и доступы в информационных системах, применение/использование которых может нанести ущерб Обществу.
Общество	Юридическое лицо, входящее в группу компаний «Северсталь».
Ответственное лицо	Работник Общества, имеющий корпоративный почтовый адрес, попадающий хотя бы под одну из следующих категорий: - линейный руководитель пользователя; - согласующий руководитель пользователя и/или его заместитель, назначенный в системе согласования доступа; - ответственный со стороны Общества за подключение работников сторонних предприятий; - диспетчер цеха; - ответственный со стороны Общества за групповую учетную запись.
Положение	Положение по управлению доступом к информационным ресурсам АО «Северсталь Менеджмент».
Пользователь	Физическое лицо, имеющее доступ к ресурсам корпоративной информационной системы Общества посредством вычислительной техники
Рабочая станция (РС)	Стационарный или мобильный компьютер, предоставленный Обществом пользователю для выполнения служебных обязанностей

Сотрудник функции ИБ	Работник Общества, в должностные обязанности которого входит организация системы управления информационной безопасностью и обеспечение ее функционирования
Телефон 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» самим пользователем или ответственными, при подписании пользователем соответствующего заявления.

5. ОСНОВНЫЕ ПОЛОЖЕНИЯ

5.1 Под управлением доступом понимается процесс наделения пользователей набором минимально необходимых полномочий, на основе их функциональных обязанностей, с целью ограничения использования ИР пользователями, не имеющими на это права.

5.2 Доступ к ИР предоставляется на основании информации, указанной в заявке и зафиксированной в соответствующей учетной системе, при условии согласования ответственными лицами

5.3 Владелец информационного ресурса, совместно с сотрудником функции ИБ и корпоративного ИТ-подразделения, определяет маршрут согласования заявок для ИР и необходимость согласования заявок сотрудниками Общества. Маршрут согласования отображается в заявке. Пересмотр маршрута осуществляется на основании заявки в учетной системе.

5.4 Владелец ИР определяет категорию информации, подлежащую защите (защищаемую информацию), допустимую для обработки с использованием этого ИР. Эта информация фиксируется в соответствующей учетной системе.

5.5 Владелец информационного ресурса с помощью соответствующей системы регистрации может определить своего заместителя, делегировав ему свои полномочия. На периоды длительного отсутствия владельца ИР (например, отпуск), заместитель должен быть определён в обязательном порядке.

5.6 Заявка должна оформляться для каждого пользователя ИР и при любом изменении прав доступа.

5.7 Набор подключаемых сервисов и уровень доступа определяется в зависимости от присвоенного признака подключаемого предприятия (контрагента). Сотрудники корпоративного ИТ-подразделения формируют и поддерживают в актуальном состоянии созданный для этой цели справочник контрагентов; при участии юридической функции присваивают подключаемому предприятию признак «корпоративная/внешняя».

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ, ИЗМЕНЕНИЯ И ПРЕКРАЩЕНИЯ ДОСТУПА К ИР

6.1 Для предоставления пользователям доступа к ИР оформляется заявка по форме, разрабатываемой индивидуально для каждого информационного сервиса или ресурса с учетом технических условий доступа.

Заявки на доступ к информационным ресурсам располагаются в электронном виде в соответствующей системе регистрации.

6.2 Если в маршруте прохождения заявки на доступ находится позиция согласования «Руководитель», то согласующий руководитель инициатора заявки определяет необходимость предоставления запрошенных прав доступа к ИР на основании функциональных обязанностей пользователя, отсутствия либо принятия потенциальных рисков несовместимых полномочий. В случае положительного решения согласовывает заявку.

6.3 Владелец ИР определяет возможность предоставления запрошенных прав доступа к ИР, руководствуясь требованием политики информационной безопасности Общества по минимизации полномочий, а также осуществляет проверку соответствия запрашиваемого уровня доступа задачам бизнеса. В случае положительного решения согласовывает заявку.

6.4 Если в маршруте прохождения заявки на доступ находится позиция согласования «ИБ», то сотрудник функции ИБ, не позднее 2 рабочих дней с момента получения запроса, проводит проверку сведений, указанных в заявке, на:

- наличие допуска к запрашиваемой информации;
- наличие подписанного соглашения о конфиденциальности;
- отсутствие рисков несовместимых полномочий;
- отсутствие противоречий с внутренними нормативными документами;
- наличие иной информации, препятствующей использование ИР заявителем;

Если при проведении проверки появляется необходимость получения дополнительной информации от инициатора заявки, то срок проверки сведений, указанных в заявке, увеличивается пропорционально сроку получению ответа от инициатора. В случае отсутствия ответа в течение 7 рабочих дней заявка отклоняется.

6.5 В случае обнаружения в заявке несоответствия условий, указанных в п. 6.2 - 6.4, заявка отклоняется с комментарием об установленном несоответствии.

6.6 Сотрудники Корпоративного ИТ-подразделения в течение временного периода,

предусмотренного регламентами предоставления сервисов, выполняют необходимые технические мероприятия для выполнения заявок. Заявки, не прошедшие регламентированную процедуру согласования, не могут быть приняты к исполнению.

6.7 Изменение прав доступа производится в связи с расширением или уменьшением основных обязанностей работника и осуществляется в порядке, установленном п. п. 6.1 – 6.6 настоящего Положения.

6.8 Прекращение доступа к ИР может быть осуществлено по требованию непосредственного руководителя пользователя, владельца/распорядителя системы или сотрудника функции ИБ. В этом случае сотрудник корпоративного ИТ-подразделения проводит блокировку доступа и фиксирует факт блокировки в информационных системах.

6.9 При получении от сотрудника заявления на увольнение работодатель имеет право прекратить/приостановить доступ к отдельным информационным ресурсам и критичным полномочиям.

7. ПОРЯДОК КОНТРОЛЯ ПРАВ ДОСТУПА К ИР

7.1 Владелец ИР обязан осуществлять периодический (не менее одного раза в год) контроль за существующими полномочиями пользователей путем сверки существующих в ИР полномочий с отраженными в заявках на доступ. Контроль полномочий пользователей осуществляется с помощью специализированного программного обеспечения, одной из функций которого является отправка уведомлений владельцу ИР о необходимости проведения проверки. Владелец ИР обязан реагировать на такие уведомления и закрывать активности в установленный срок.

7.2 Сотрудник функции ИБ осуществляет контроль за соответствием текущей конфигурации подсистемы управления доступом к ИР утвержденным заявкам на предоставление/изменение/прекращение доступа к ИР.

7.3 Сотрудник функции ИБ осуществляет контроль правильности предоставления прав доступа.

7.4 В случае выявления расхождений между существующими полномочиями пользователей и информацией в утвержденных заявках, сотрудник функции ИБ проводит расследование в соответствии с действующими нормативными документами.

8. ЖИЗНЕННЫЙ ЦИКЛ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

8.1 В зависимости от используемых пользователем ИС и способа аутентификации в них (локальная УЗ, УЗ домена КСПД, УЗ домена ТСПД), пользователю могут создаваться соответствующие учетные записи.

8.2 Перед созданием любой учетной записи пользователь должен быть ознакомлен с нормативными актами в области ИТ и ИБ. Факт ознакомления фиксируется:

- в бумажном виде в листе регистрации ознакомления/ответственности (приложение №1), копия которого прикрепляется к заявке;
- в электронном виде в отдельной форме специализированной информационной системы.

Оригинал листа ознакомления хранится:

- в кадровой службе предприятия, если пользователь является работником предприятия;
- у инициатора заявки, если пользователь является внешним лицом.

8.3 Учетная запись пользователя должна обладать признаками уникальности, позволяющими однозначно идентифицировать использующего ее лицо, в период работы пользователя и не повторять свойства архивных учетных записей. Имя учетной записи пользователя формируется с использованием латиницы. Транслитерация кириллицы в латиницу производится на основании рекомендаций Раздела IV части 1 международного стандарта ИКАО Doc 9303.

8.4 Для работы с ИС, при аутентификации в которых используются учетные записи домена КСПД, пользователю создается уникальная персональная учетная запись в соответствующем домене КСПД. Создание учетной записи работнику предприятия, оформленному по трудовому договору или по договору гражданско-правового характера (ГПХ), происходит по проставленному кадровой службой коду мероприятия в системе SAP HCM, или по заявке от кадровой службы предприятия, учет персонала которого ведется в иных системах.

Учетная запись для работника предприятия, работающего по договору ГПХ, должна иметь ограничения по сроку использования, который определяется в SAP HCM.

8.5 Для работы с ИС, при аутентификации в которых используются учетные записи домена ТСПД, пользователю может быть создана дополнительная учетная запись в соответствующем домене ТСПД.

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

8.7 Учетная запись для внешнего пользователя может быть создана по заявке от любого пользователя. К заявке необходимо приложить скан-копии документов, перечень которых приведен в приложении 2. Заявка должна быть согласована с ответственным за процесс, в рамках которого создается учетная запись, и с сотрудником функции ИБ. При создании такой учетной записи устанавливается ограничение по сроку использования, который может быть определен инициатором заявки. Ограничение по сроку использования данной категории учетной записи должно учитывать срок действия договора, в рамках которого создается данная учетная запись, или период в один год, в зависимости от того, что наступит раньше. При необходимости продления срока действия такой учетной записи следует зарегистрировать соответствующую заявку.

8.8 Учетная запись пользователя в КИС должна блокироваться в течение 1 календарного дня, в который наступили следующие события:

а. истечение срока действия учетной записи;
б. увольнение работника без последующего приема внутри ГК «Северсталь»;
в. перевод работника предприятия на легкий труд, уход в отпуск по беременности и родам или отпуск по уходу за ребенком;
г. приостановление действия трудовых договоров с работниками, призванными на военную службу по мобилизации в Вооруженные Силы Российской Федерации;
д. переход работника в другое юридическое лицо группы компаний «Северсталь»;
е. отстранение от работы (недопущение к работе) по причинам, предусмотренным законодательством;
ж. по требованию сотрудника функции ИБ.

8.9 В случае перевода работника в другое подразделение текущий непосредственный руководитель обязан принять решение о сохранении или отзыве существующих полномочий учетной записи работника,

8.10 В случае необходимости сохранения полномочий учетной записи при наступлении событий, указанных в п. 8.8 (за исключением подпунктов «г», «д», «е» и «ж»), ответственное лицо создает соответствующий запрос на сохранение уровня полномочий учетной записи, согласование которого происходит по маршруту, созданному в соответствии с условиями п. 5.3.

8.11 Полномочия заблокированной учетной записи при наступлении события подпункта «д» п. 8.8 могут быть переназначены на создаваемую учетную запись работника по новому месту работы. Переназначенные полномочия доступа должны быть подтверждены участниками маршрутов согласования заявки на доступ к информационным ресурсам в течении 14 календарных дней, по истечении которых неподтвержденные полномочия отзываются автоматически.

8.12 В случае массовых переходов работников в другое юридическое лицо группы компаний «Северсталь» с сохранением функциональных обязанностей (кадровой службой проставлен соответствующий код мероприятия в учетной системе или создана заявка на массовый переход), учетная запись работника не блокируется и существующие полномочия доступа не отзываются.

8.13 Заблокированная учетная запись при наступлении событий подпунктов «е» и «ж» п. 8.8 может быть разблокирована только при устранении условий возникновения блокировки.

8.14 Учетная запись может быть заблокирована по мотивированному требованию непосредственного руководителя. В этом случае сотрудник корпоративного ИТ-подразделения проводит блокировку и фиксирует факт блокировки в информационных системах.

8.15 Учетная запись пользователя должна быть заблокирована автоматически по истечении 14 календарных дней с момента ее создания, если им не будет пройдено обязательное обучение:

- Для работников компании - электронный курс «Первичный инструктаж по ИБ» на портале «Мое обучение и развитие».

8.16 Использование групповой учетной записи не допускается для ИР с защищаемой информацией, поддерживающих дополнительную персональную идентификацию

пользователей. В особых случаях (например, для обеспечения непрерывного технологического процесса) допускается использование групповой учетной записи несколькими работниками.

8.17 Каждая групповая учетная запись должна иметь владельца, назначение которого согласуется руководителем подразделения данного работника. Любые изменения, касающиеся данной учетной записи, должны согласовываться с ее владельцем.

8.18 В случае использования групповой учетной записи, Корпоративное ИТ-подразделение обеспечивает:

- учет владельцев групповой учетной записи и их периодическую (не менее 1 раз в 6 месяцев) инвентаризацию;
- наличие информации в учетной системе о персональных учетных записях всех работников, заявленных к использованию конкретной групповой учетной записи;
- запуск процедуры смены пароля от групповой учетной записи в случае наступления событий, перечисленных в п. 8.8 в отношении владельца групповой учетной записи;
- учет групповой учетной записи и оборудования/ИР, на котором она будет использоваться.

8.19 Владелец групповой учтённой записи обязан осуществлять периодический (не менее одного раза в год) контроль за перечнем пользователей, имеющих доступ к групповой учетной записи. Контроль за перечнем пользователей осуществляется с помощью специализированного программного обеспечения, одной из функций которого является отправка уведомлений владельцу групповой учетной записи о необходимости проведения проверки. Владелец групповой учетной записи обязан реагировать на такие уведомления и закрывать активности в установленный срок.

8.20 Учетная запись пользователя блокируется в случае, если она не используется в течение 180 календарных дней

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

8.18 Корпоративное ИТ-подразделение обязано сохранять в течение 3 лет информацию об удаленной учетной записи, содержащую реквизиты доступа в корпоративный домен (уникальные идентификаторы, в т. ч. дату и время удаления).

9. ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ ПАРОЛЯМИ

9.1 Требования к средствам аутентификации установлены в Политике парольной защиты группы компаний «Северсталь», утверждаемой и вводимой в действие приказом руководителя Общества.

9.2 Изменение пароля учетной записи осуществляется:

- пользователем-владельцем самостоятельно;
- в случае необходимости принудительного изменения – по заявке от сотрудника функции ИБ.

9.3 Передача первичного пароля пользователю осуществляется следующими способами:

- SMS на телефонный номер для SMS-информирования;
- корпоративная электронная почта;
- запечатанный конверт.

9.4 Выбор способа передачи первичного пароля пользователя определяется по следующему алгоритму:

а) отправить SMS- на телефонный номер для SMS-информирования;

б) если отправка SMS не возможна (телефонный номер не указан или не актуален, либо SMS-сообщение не доставлено адресату), то пароль отправляется на корпоративный электронный почтовый адрес пользователя;

в) если у пользователя отсутствует корпоративный электронный почтовый адрес или отсутствует возможность доступа к нему, то пароль отправляется на корпоративный электронный почтовый адрес ответственного лица, указанного в заявке.

г) пароль от групповой учетной записи отправляется на корпоративный электронный почтовый адрес ответственного лица, указанного в заявке;

д) если использование технических каналов невозможно, то передача пароля осуществляется непосредственно пользователю на бумажном носителе в запечатанном конверте.

9.5 Не допускается хранение паролей и иных кодов для проверки подлинности учетной записи пользователя в открытом виде без применения средств защиты (программное

обеспечение для хранения паролей (KeePass) в электронном виде, принятое к использованию в ГК «Северсталь»; запираемые металлические шкафы или сейфы для хранения паролей на бумажном носителе в запечатанном конверте).

10. ОРГАНИЗАЦИЯ УДАЛЕННОГО ДОСТУПА

10.1 Удаленный доступ в КИС предоставляется сотрудникам, на основании заявки зарегистрированной в соответствующей учтённой системе, при условии согласования ответственными лицами.

10.2 Организация удаленного доступа в КИС осуществляется с применением средств многофакторной аутентификации (сертификат PKI, код из приложения, Push-уведомления, OTP, SMS). Для работников Общества, категории которых перечислены в Приложении 3, доступ организуется только с применением сертификата PKI, записываемого на физический носитель в защищённом исполнении.

10.3 Удаленный доступ не предоставляется для сотрудников спец. подразделений, а также для HR-сотрудников, ведущих воинский учет.

10.4 Организация любых ИТ-сервисов, использующих технологии удаленного доступа в КИС, осуществляется Корпоративным ИТ-подразделением.

10.5 Установка и настройка программного обеспечения, необходимого для удаленного доступа в КИС, на корпоративное оборудование осуществляется специалистами Корпоративного ИТ-подразделения.

10.6 Выбор типа удаленного подключения к КИС осуществляется согласно Приложению 4.

10.7 Каждый сеанс удалённого доступа должен проходить повторную аутентификацию.

10.8 Для информационных ресурсов и информационных систем, к которым предоставляется удаленный доступ, необходимо включить журнал аудита событий. В журналах должны быть отражены время начала и завершения сеанса удалённого ,подключения, сетевой адрес источника и назначения, тип подключения, идентификатор пользователя и идентификатор устройства, с которого выполнено подключение.

10.9 Все удалённые соединения должны ограничиваться средствами разграничения сетевого доступа, контролироваться средствами защиты информации.

11. ОТВЕТСТВЕННОСТЬ

11.1 Ответственное лицо несет ответственность за:

- соблюдение порядка предоставления, изменение, прекращения доступа;
- конфиденциальность передаваемого через него пароля пользователя;
- идентификацию пользователя при передаче ему пароля.

11.2 Пользователь несет ответственность за:

- конфиденциальность своих паролей;
- своевременную актуализацию своих контактных данных используемых для получения или восстановления пароля;
- смену первичного пароля учетной записи;
- полноту и достоверность предоставленной информации в заявке.

11.3 Сотрудник Корпоративного ИТ-подразделения несет ответственность за сохранение конфиденциальности данных, созданных для первичной идентификации пользователя в системе.

11.4 Сотрудник функции ИБ несет ответственность за своевременную обработку поступающих инцидентов, согласно принятым в Обществе правилам по управлению инцидентами информационной безопасности.

11.5 Владелец информационного ресурса несет ответственность за принятие решений по вопросам создания и ликвидации ресурса, определение правил доступа пользователей к ресурсу с учетом принципа минимально необходимых полномочий и допустимых рисков.

11.6 Владелец групповой учетной записи несет ответственность за своевременное информирование корпоративного ИТ - подразделения об изменениях в составе работников, использующих соответствующую групповую учетную запись.

11.7 Непосредственный руководитель пользователя при согласовании доступа несет ответственность за соответствие запрошенного набора прав доступа к ИР, отраженного в заявке, функциональным обязанностям пользователя с учетом принципа минимально необходимых полномочий и допустимых рисков.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

12.2 Если в результате изменения законодательства отдельные положения настоящего Положения 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.

Приложение 1

_____

_____

(наименование компании/дирекции)

_____

_____

(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	Инструкции пользователя корпоративной информационной системы группы компаний «Северсталь».		
5	Положение по управлению доступом к информационным ресурсам группы компаний «Северсталь»		

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

номер телефона

_____

(подпись пользователя)

Личную подпись пользователя УДОСТОВЕРЯЮ

_____

_____ _____

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

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

Приложение 2

Перечень предоставляемых документов

Группа пользователей	Предоставляемые документы
Внешний пользователь (не работник Общества)	1. Лист регистрации ознакомления / ответственности пользователя 2. Обоснование создания учетной записи (ссылка на договор, протокол, распоряжение 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

Перечень категорий работников, 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. Сотрудники бизнес-единиц: ООО «Северсталь-ЦЕС», АО «Северсталь-Инфоком», ООО «Северсталь Диджитал», ООО «Северсталь-СКИФ», ООО «Делетрон».
5. Сотрудники подразделений: СОБ, УРМиВК, УВА, финансовой функции.
6. Сотрудники и подрядчики, занимающиеся наладкой и обслуживанием информационных систем и оборудования на объектах критической информационной инфраструктуры.
7. Сотрудники, занимающиеся сопровождением инфраструктуры АСУ ТП (сетей, контроллеров, серверов, рабочих станций).
8. Сотрудники, имеющие доступ к строго конфиденциальной информации, биометрическим и специальным категориям персональных данных.
9. Сотрудники, работающие с системами банк-клиент.
10. Внешние подрядчики, осуществляющие разработку и поддержку информационных сервисов и систем.

Приложение 4

Виды удаленного доступа

Вид удаленного доступа	Ресурсы для доступа	Вид устройства	Тип пользователя
Доступ к ИТ-ресурсам из Интернет с корпоративных ноутбуков или ПК (VPN-Corp)	Ресурсы объявленные общекорпоративными	Корпоративные	Корпоративный
VPN-Util-<код_проекта>	Доступ к отдельно взятому ресурсу (списку ресурсов)	Корпоративные и некорпоративные	Корпоративный, некорпоративный
VPN-Adm-<код_проекта (процесса)>	Ресурсы объявленные общекорпоративными и дополнительные заявленные ресурсы	Корпоративные	Корпоративный
Доступ к ИТ-ресурсам из Интернет (на терминал RDSFarm-Corpusers)	Ресурсы объявленные общекорпоративными	Корпоративные и некорпоративные	Корпоративный
Доступ к ИТ-ресурсам из Интернет для некорпоративных пользователей (RDSFarm-ExtUsers)	Ограниченный список корпоративных ресурсов	Некорпоративные	Некорпоративный
Доступ к ИТ-ресурсам из Интернет для доступа к SAP внешних разработчиков (stal-rds-dev)	Ограниченный список корпоративных ресурсов	Корпоративные и некорпоративные	Корпоративный, некорпоративный
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
Удаленный доступ к ИТ-ресурсам из Интернет по RDP до windows сервера через шлюз удаленных рабочих столов (RDGW)	Специализированные ресурсы	Корпоративный, некорпоративный	Корпоративный, некорпоративный
Удаленный доступ к ИТ-ресурсам из Интернет через	Специализированные ресурсы	Корпоративные и некорпоративные	Корпоративный, некорпоративный

шлюз мониторинга (PAM)			
Удаленный доступ к ИТ-ресурсам из Интернет через виртуальное рабочее место (VDI)	Ресурсы объявленные общекорпоративными, специализированные ресурсы	Корпоративные и некорпоративные	Корпоративный, некорпоративный