Приложение № 1

к Приказу Генерального директора

АО «Северсталь Менеджмент»

№ ОРД/СМ/П-15-0000224 от «24» июня 2015 г.

ПОЛИТИКА АО «СЕВЕРСТАЛЬ МЕНЕДЖМЕНТ» В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Редакция 1

Цель политики

Предотвращение и минимизация потерь АО «Северсталь Менеджмент» и управляемых им обществ от:

- Утечек конфиденциальной информации;
- Использования недостоверной, искаженной информации;
- Нарушения процессов обработки информации.

Наши обязательства

Информация, представляющая ценность для бизнеса и клиентов, защищается вне зависимости от способов ее обработки.

Направления деятельности

- Создание, поддержка и развитие системы управления информационной безопасностью (СУИБ), соответствующей требованиям бизнеса, законодательства и лучшим мировым практикам.
- Прогнозирование, предупреждение, выявление, противодействие и нейтрализация внешних и внутренних угроз информационной безопасности, а также минимизация ущерба от их воздействия.
- Реализация комплекса мероприятий по обеспечению безопасности информационных систем, персонала, инфраструктуры, сетей передачи данных и носителей информации.
- Обеспечение выполнения и контроль соблюдения требований законодательства и локальных нормативных актов в области информационной безопасности.
- Повышение осведомленности персонала в вопросах, относящихся к информационной безопасности.

Наши принципы

- **Бизнес-ориентированность.** СУИБ должна соответствовать целям и ценностям бизнеса, и защищать его интересы.
- **Системность.** Организационные меры и технические средства должны раз-

рабатываться и применяться в рамках единой системы защиты, учитывающей все способы реализации актуальных угроз и не содержащей слабых мест на стыке отдельных ее компонентов.

- **Непрерывность.** Процессы, связанные с обеспечением информационной безопасности, должны выполняться на всех этапах жизненного цикла информации - от создания до уничтожения. Каждый работник на своем уровне должен принимать участие в этих процессах.
- **Своевременность.** Меры обеспечения защиты информации должны носить упреждающий характер.
- **Постоянное совершенствование.** СУИБ должна развиваться и совершенствоваться в соответствие с появлением новых векторов распространения угроз, изменениями в корпоративной информационной системе и нормативных актах, учитывать требования законодательства и опираться на достигнутые результаты и лучшие мировые практики в области защиты информации.
- **Экономическая целесообразность.** Затраты на поддержку и развитие СУИБ не должны превышать размер ущерба от разглашения, утраты, уничтожения, искажения и несанкционированного доступа к информации.
- **Минимизация полномочий.** Доступ к информационным ресурсам и технологиям должен быть ограничен, обоснован и предоставляться исключительно для выполнения служебных обязанностей.
- **Контроль.** Информационные ресурсы и средства коммуникаций должны предусматривать механизмы контроля порядка обращения с конфиденциальной информацией.
- **Законность.** СУИБ должна соответствовать требованиям законодательства.