Общество с ограниченной ответственностью «НовосибирскНИПИнефть»	Соответствует ПР 50-732-93 **УТВЕРЖДАЮ**
г. Новосибирск	Генеральный директор
ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	**Г.А.Борисов**
	«23» июня 2015 года м.п.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность

Цели и задачи

Осуществление деятельности компании связано с управлением информацией, являющейся важным активом ООО «НовосибирскНИПИнефть», далее «Компании», и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.

Ответственность

Руководство Компании осуществляет общее управление информационной безопасностью и обеспечивает необходимые условия для: реализации мероприятий по оценке рисков информационной безопасности и защиты информации; поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью; регулярного обучения сотрудников в сфере информационной безопасности руководству.
Сотрудники компании несут персональную ответственность за соблюдение требований настоящего документа, и обязаны сообщать обо всех нарушениях в области информационной безопасности.
В трудовых договорах и должностных инструкциях работников устанавливается ответственность сотрудников за сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения своих обязанностей.

Управление информационной безопасностью

Настоящая политика соответствует международному стандарту ISO/IEC 27001:2005; требованиям законодательства Российской Федерации, нормативным и договорным обязательствам ООО «НовосибирскНИПИнефть», с точки зрения информационной безопасности.
Все информационные активы ООО «НовосибирскНИПИнефть», включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, подлежат учету и категорированию в соответствии с их важностью и степенью доступа.
В соответствии с установленными процедурами в области управления рисками осуществляется регулярная оценка рисков информационной безопасности. При ее проведении учитывается вероятность угроз информационной безопасности и степень их влияния на бизнес-процессы, финансовое состояние и деловую репутацию ООО «НовосибирскНИПИнефть»,
По результатам оценки рисков информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения безопасности.
Сотрудники ООО «НовосибирскНИПИнефть», получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей. Руководство проводит информирование, обучение и повышение квалификации работников в сфере информационной безопасности.
Регламенты обращения с информацией описаны специальных приказах, являющихся, в свою очередь внутренними документами компании.

Общие положения

- Всю деловую переписку вести только с персонального служебного почтового ящика;
- Все деловые контакты (включая встречи, деловая переписка, звонки) согласовываются непосредственно с руководителем.
- Перед отправкой любого рода материалов проверить руководителю соответствие адресата назначению;
- Служебные стационарные компьютеры подключаются к внутренней сети проводным способом, беспроводное подключение только через гостевую сеть, не связанную с локальной;
- Гостевая беспроводная сеть описана в разделе «Гостевая беспроводная сеть»
- Набор программного обеспечения на рабочих компьютерах – см. раздел «Список минимального набора программного обеспечения» – по согласованию с системным администратором и руководством по запросу;
- Любые изменения в конфигурации служебного компьютера или учетных записях, требующие взаимодействия с системным администратором, производятся только по согласованию с руководством;
- Хранение данных на сервере описано в разделе «Хранение данных на сервере»;
- Внешний доступ к серверу описываемый в разделе «Внешний доступ к серверу», используется исключительно для получения данных Заказчика**»**;
- Системный администратор должен обеспечить раздельное хранение данных, полученных от разных Заказчиков, а также проектных файлов;
- Запрещено выносить за пределы офиса рабочие файлы, на внешних носителях (USB-флеш, оптические диски и т.д.);
- Материалы по проекту, передаваемые Заказчику в ходе очной защиты, следует записывать на чистый носитель, содержащий только материалы, относящиеся непосредственно к защите проекта;
- При отправке Заказчику каких-либо образцов и т.д. упаковывать следует в специально подготовленную чистую бумагу, использование черновиков и т.п. не допускается;
- Любые бумажные носители, утратившие свою ценность, подлежат обязательному уничтожению в шредере, использование мусорных корзин для утилизации не допускается;
- Всю работу над текущим проектом в обязательном порядке сохранять на сервере в конце рабочего дня, в соответствии с инструкцией в разделе «**Хранение данных на сервере**».

Список минимального набора программного обеспечения

1. ОС – Microsoft Windows 7 SP1.
2. Офисный набор – Microsoft Office 2007 (Word, Excel, Power Point, Outlook).
3. Просмотр и создание PDF документов – Adobe Acrobat 11.
4. Просмотр и редактирование изображений – ACDSee Pro 8, Adobe Photoshop CS2, Corel Draw x6.
5. Оптическое распознавание документов – ABBY Finereader 11.
6. Электронный словарь – ABBY Lingvo x5.