УТВЕРЖДАЮ:

Генеральный директор
ЗАО «ИНФАПРИМ»

_____ Трофимов Г. А.
"09" января 2014 г.

ПОЛОЖЕНИЕ
о компьютерной безопасности и правилах пользования информационно-техническими ресурсами ЗАО «ИНФАПРИМ»

1. Общие положения.

1.1. Настоящее положение призвано гарантировать надлежащее использование компьютеров и телекоммуникационных ресурсов сотрудниками ЗАО «ИНФАПРИМ».

1.2. В целях обеспечения нормального функционирования информационно-технических ресурсов (далее ИТ-ресурсы) ЗАО «ИНФАПРИМ» пользователь обязан соблюдать данное положение.

1.3. ИТ ресурсы, а так же вся хранимая на машинных носителях информация и конечные данные являются собственностью ЗАО «ИНФАПРИМ».

2. Обязанности руководителей

2.1. Руководители структурных подразделений обязаны обеспечивать строгое соблюдение настоящего положения.

2.2. Руководители структурных подразделений обязаны заранее уведомлять ИТ отдел об увольнении, принятии на работу, отпуске, перемещениях внутри отдела или ГК и других изменениях в штатном расписании.

2.3. Руководители структурных подразделений обязаны сделать в ИТ обоснованную заявку для обеспечения сотрудников своего подразделения аппаратными и программными средствами, необходимыми для работы, а так же доступа к ресурсам сети Интернет и индивидуальным электронным почтовым ящикам.

3. Правила доступа к ресурсам Интернет и работы с электронной почтой.

3.1. Доступ в Интернет предоставляется с санкции начальника структурного подразделения для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам деятельности.

3.2. Каждый пользователь ИТ ресурсов получает персональный электронный адрес. Вся переписка должна вестись строго с использованием этого электронного адреса.

3.3. Пользуясь электронной почтой и ресурсами Интернета с рабочего места, сотрудник выступает от имени компании, а не как частное лицо, и потому соблюдает принципы делового общения и этикета.

3.4. Запрещается передавать по электронной почте конфиденциальную информацию (электронная почта не является средством, гарантирующим защиту информации от доступа третьих лиц).

4. Правила доступа к сетевым ресурсам компании.

4.1 Общие сетевые файловые ресурсы на серверах компании, создаются по заявлению от руководителя структурного подразделения. Заявление должно содержать в себе сетевое

имя ресурса, список пользователей, с указанием типа доступа (полный\чтение) для каждого пользователя.

4.2 Доступ сотруднику компании, к сетевому файловому ресурсу предоставляется на основании служебной записки от руководителя структурного подразделения, подтвержденной ответственным за этот сетевой ресурс. Ответственным за сетевой ресурс, является сотрудник, инициировавший создание данного ресурса, либо по согласованию любой другой сотрудник.

4.3 Доступ сотруднику к базам 1С предоставляется на основании служебной записки, от руководителя структурного подразделения, на имя руководителя информационно аналитического департамента.

5. Положения о программном обеспечении

5.1. Список пользовательского ПО, устанавливаемого на рабочие станции:

- 7zip – архиватор;
- Office standart – офисный пакет, включает в себя word, excel, powerpoint, outlook;
- Foxit Reader (либо adobe reader) – программа для чтения pdf файлов;
- Антивирус
- Antimalware – программа для поиска spyware;
- CCleaner – программа для оптимизации компьютера;
- MyDefrag – дефрагментатор.

5.2. Дополнительное ПО устанавливается на основании служебной записки от сотрудника, подтвержденной руководителем структурного подразделения. Служебная записка должна содержать обоснованную служебную необходимость установки данного ПО.

6. Привилегированный доступ к локальному компьютеру.

6.1. Административные права на локальную рабочую станцию предоставляются на основании служебной записки, от сотрудника, подтвержденной руководителем структурного подразделения. Служебная записка должна содержать обоснованную служебную необходимость в предоставления администраторских полномочий на локальную рабочую станцию.

7. Права и обязанности.

7.1. Пользователь ИТ ресурсов имеет право:

- Требовать от руководства компании обеспечить бесперебойную работу вычислительной техники, ЛВС и основных программных продуктов (операционной системы MS Windows, пакета офисных программ “MS Office”, почтовых клиентов, интернет-браузеров).
- Требовать у начальника своего отдела (структурного подразделения) установки необходимых для работы программных продуктов или аппаратного обеспечения.

7.2. Пользователь ИТ ресурсов обязан:

- Входить в сеть при каждом сеансе работы с использованием персонального пароля и имени пользователя.
- Хранить служебную информацию, на локальной рабочей станции, в папках «Мои Документы» и «Рабочий Стол», если нет потребности хранения данной информации на сетевых дисках.
- Осуществлять смену пароля для своей учетной записи, в соответствии с политиками сетевой безопасности компании.
- Осуществлять своевременное резервное копирование принадлежащих ему файлов и баз данных в соответствии с инструкцией.
- Информировать своего руководителя при обнаружении вирусов, попыток несанкционированного доступа или каких-либо подозрительных действий.

- При проведении работ, предполагающих интенсивную загрузку ЛВС (скачивание большого количества данных, большое количество сетевых соединений), поставить в известность своего руководителя.

7.3. Пользователю ИТ ресурсов запрещается:

- Устанавливать, модифицировать или хранить на машинных носителях любое программное обеспечение без согласования с руководителем.
- Самостоятельно разбирать системный блок или проводить работы по установке или обслуживанию любых других аппаратных средств.
- Передавать кому бы то ни было свой пароль, а так же хранить свой пароль в легкодоступном месте и в явной форме.
- Допускать к своему компьютеру других пользователей для любого рода деятельности без согласования с руководителем.
- Использовать доски объявлений, конференций с применением имен пользователей и паролей внутренней сети, в личных целях, для переговоров с друзьями и членами семьи.
- Запрашивать и получать из Интернета программные продукты, мультимедийные данные или изображения, кроме случаев, связанных с производственной необходимостью.
- При работе с электронной почтой запрещается открывать сообщения сомнительного содержания, или пришедшие от неизвестного отправителя.
- Использовать любые программные и аппаратные средства, которые могут привести к перегрузке сети или иным способом негативно повлиять на ее работу.
- Использовать программы подбора паролей пользователей других компьютеров сети, сканирования адресов других пользователей, подделки служебной информации о компьютере, поиск уязвимостей на серверах компьютерной сети.
- Использовать программы выявления неисправности конфигураций других компьютеров и устройств, подключенных к сети.
- Использование интернет-пэйджеров SMS и подобных программ таких как ICQ, Odigo, IRC, AOL, Miranda и т.п.
- Вносить изменения в файлы, не принадлежащие самому пользователю.
- Разрабатывать или распространять любые виды компьютерных вирусов, "троянских коней" или "логических бомб".
- Использовать компьютеры для любых видов противозаконной деятельности.

8. Ответственность.

8.1. Пользователь несет ответственность за целостность и сохранность полученного оборудования.

8.2. Пользователь несет полную ответственность за все действия, совершенные от его имени, с использованием его учетной записи.

8.3. При несоблюдении пользователями условий настоящей инструкции к ним применяется административные меры наказания, вплоть до увольнения, в соответствии со степенью вины, установленной служебным расследованием.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно.

9.2. Текст настоящего Положения подлежит доведению до сведения сотрудников ЗАО «ИНФАПРИМ».