Приложение № 9 к Политике информационной безопасности в ООО «ФанДог», утвержденной Приказом Генерального директора ООО «ФанДог» №9 от «03» апреля 2023 г.

Инструкция пользователя по соблюдению режима информационной безопасности

1. Общие требования

1.1 При работе с информационными ресурсами Компании каждый сотрудник обязан:

- обеспечивать, исходя из своих возможностей и специальных обязанностей по обеспечению безопасности информации, защиту от несанкционированного доступа к информации, к которой он имеет санкционированный доступ в силу своих служебных обязанностей;
- ни в какой форме не участвовать в процессах несанкционированного доступа к информации, принадлежащей другим сотрудникам и службам;
- ни в какой форме не использовать ставшую ему известной в силу исполнения своих функциональных обязанностей информацию не по прямому назначению;
- при нарушении установленных правил доступа другими сотрудниками сообщать об этом непосредственному начальнику, ответственным администраторам или в Службу безопасности.

1.2 Ремонтные и профилактические регламентные работы должны производиться только уполномоченными лицами эксплуатационной службы по согласованию с руководителем (ответственным лицом) подразделения, в котором установлено компьютерное оборудование. Порядок снятия, переноса, модификации аппаратной конфигурации устанавливается Регламентом проведения такого рода работ и осуществляется только уполномоченными лицами службы АХО.

2. Работа в автоматизированной информационной системе

2.1 При работе в автоматизированной информационной системе Компании пользователь обязан:

- сохранять в тайне пароли доступа к системе (системам);
- надежно хранить физические ключи (идентификаторы) доступа;
- периодически изменять личные пароли, если это предписано регламентом управления доступом;
- при случайном получении (сбой механизмов защиты, аварии, небрежность персонала и др.) доступа к чужой конфиденциальной информации прекратить какие-либо действия в системе и незамедлительно сообщить в Службу безопасности и администратору системы;
- сообщать в службу безопасности и администратору системы об известных каналах утечки, способах и средствах обхода или разрушения механизмов защиты.

2.2 При работе в автоматизированной информационной системе Компании пользователю запрещается (кроме особо оговоренных случаев):

- записывать в любом доступном виде или произносить вслух известные пользователю пароли;
- регистрироваться и работать в системе под чужим идентификатором и паролем;
- передавать идентификаторы и пароли кому бы то ни было;
- оставлять без контроля рабочее место в течение сеанса работы;
- позволять производить любые действия с закрепленным за пользователем комплектом программно-аппаратных средств другим лицам;
- несанкционированно изменять или уничтожать данные или программы в сети или на внешних (отчуждаемых) носителях;

- оставлять без контроля носители критичной информации;
- использовать компьютерную технику в нерабочее время не по прямому назначению;
- заниматься исследованием вычислительной сети;
- игнорировать системные сообщения и предупреждения об ошибках;
- несанкционированно устанавливать на автоматизированные рабочие места любые дополнительные программные и аппаратные компоненты и устройства;
- копировать на съёмные носители любое программное обеспечение и файлы данных;
- использовать для передачи информации ограниченного доступа не предназначенные для этого средства и каналы связи.