УТВЕРЖДАЮ
Директор ГКУ ТО «ЦИТТО»

_____А. Р. Усманов

«__30__» _____марта_____ 2018 г.

ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОМУ РАБОЧЕМУ МЕСТУ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ДЕЛОПРОИЗВОДСТВА»

2018

1. Общие положения

Настоящие требования разработаны в целях организации обеспечения информационной безопасности на автоматизированном рабочем месте пользователя (далее – АРМ), при работе в информационной системе «Система электронного документооборота и делопроизводства», введенной в эксплуатацию Распоряжением Правительства Тюменской области от 23.04.2012 № 636-рп «О введении в эксплуатацию системы электронного документооборота и делопроизводства» (далее — ИС СЭД).

Предъявляемые требования являются обязательными для всех АРМ, с которых ведется обработка персональных данных в ИС СЭД, в исполнительных органах государственной власти Тюменской области, государственных унитарных предприятиях, государственных учреждениях и автономных некоммерческих организациях Тюменской области, координацию, регулирование и контроль финансово-хозяйственной деятельности которых осуществляют исполнительные органы государственной власти Тюменской области; иных государственных органах власти, органах местного самоуправления, муниципальных унитарных предприятиях, муниципальных учреждениях и автономных некоммерческих организациях, координацию, регулирование и контроль финансово-хозяйственной деятельности которых осуществляют органы местного самоуправления Тюменской области, и в иных хозяйствующих субъектах, присоединившихся к ИС СЭД на основании соглашения об организации информационного взаимодействия в соответствии с Регламентом, размещенным на сайте Оператора ИС СЭД (citto.ru).

Требования могут дополнятся в соответствии с нормативно-правовыми актами Российской Федерации, регламентирующими обеспечение безопасности персональных данных.

2. Требования к АРМ

1. Установлена лицензионная версия операционной системы;
2. Для операционной системы должны быть установлены актуальные обновления в части информационной безопасности;
3. Установлено лицензионное средство антивирусной защиты сертифицированное в Российской Федерации, с актуальными базами вирусных сигнатур (Kaspersky Endpoint Security, Dr.Web, или другое) ;
4. Установлено, в случае обработки на АРМ пользователя персональных данных, сертифицированное в Российской Федерации, средство защиты от несанкционированного (в том числе случайного) доступа к информации (например Dallas Lock или другое);
5. Выход в интернет с АРМ пользователя должен осуществляться с использованием межсетевого экрана (например VipNet, Континент, UserGate или другое);
6. Установлено (в случае необходимости) сертифицированное средство криптографической защиты информации (например VipNet Client или КриптоПро);

7. При работе на АРМ должны быть выполнены иные требования к обеспечению информационной безопасности, предусмотренные законодательством РФ.

3. Ответственность

Ответственность за соблюдение настоящих требований возлагается на Администратора информационной безопасности конкретной организации осуществляющей ведение документооборота посредством ИС СЭД.