Приложение № 1
к распоряжению администрации
округа «Усинск»
от 11 июня 2025 г. № 111-р

ФОРМА
раздела должностной инструкции сотрудников администрации муниципального округа «Усинск» Республики Коми, имеющих доступ к персональным данным

1. К конфиденциальной информации администрации муниципального округа «Усинск» Республики Коми (далее – Администрация) относится: служебная информация Администрации, персональные данные субъектов персональных данных Администрации. Перечень конфиденциальной информации содержится в Перечне персональных данных, обрабатываемых в Администрации. Порядок обращения с такой информацией регулируется Положением об обработке персональных данных, Политикой обработки персональных данных, Инструкцией пользователя информационных систем персональных данных и Инструкцией ответственного за организацию обработки персональных данных, утвержденных распоряжением главы муниципального округа «Усинск» Республики Коми.

2. В период работы и (или) срока договорных отношений с Администрацией (либо бессрочно, если не указан срок) после окончания таких отношений:

2.1.Сотрудник обязан:

− выполнять требования действующего законодательства Российской Федерации, распоряжений, инструкций, положений и иных локальных нормативных актов Администрации по обеспечению сохранности конфиденциальной информации;

− не разглашать и не передавать конфиденциальные сведения, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей;

− не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично конфиденциальные сведения без соответствующего разрешения главы муниципального округа «Усинск» Республики Коми – главы администрации (собственника информации) (далее – глава округа «Усинск») в установленных им объемах;

− не использовать конфиденциальные сведения при осуществлении иной деятельности, которая в качестве конкурентного действия может нанести ущерб Администрации;

− при санкционированной передаче конфиденциальной информации по незащищенным каналам связи, в том числе сети Интернет, пользоваться шифровальными (криптографическими) средствами;

− во время работы с документами, содержащими конфиденциальную информацию, исключать несанкционированное ознакомление с их

содержимым посторонними лицами. После окончания работы с такими документами – убирать их в сейф (хранилище);

− хранить в тайне личные ключи и атрибуты доступа (пароли) к помещениям, хранилищам, сейфам и ресурсам информационной системы Администрации;

− при отсутствии визуального контроля за рабочей станцией (оставление рабочего места на любой промежуток времени) немедленно заблокировать доступ к компьютеру. Для этого необходимо нажать одновременно комбинацию клавиш [Ctrl][Alt][Del] и выбрать опцию <Блокировка> или использовать комбинацию клавиш [WIN][L];

− незамедлительно, в кратчайшие сроки, сообщить главе округа «Усинск» об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальных сведений;

− в случае попытки посторонних лиц получить конфиденциальные сведения, немедленно сообщить об этом главе округа «Усинск»;

− нести ответственность, если действия или бездействия сотрудника повлекут за собой разглашение конфиденциальной информации, в соответствие с законодательством Российской Федерации и локальными нормативными актами Администрации;

− при прекращении работ (трудовых отношений) все материальные носители, содержащие конфиденциальную информацию (флэш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать непосредственному руководителю;

− использовать информационные ресурсы Администрации и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

2.2.Сотруднику запрещается:

− самостоятельно, без согласования с администратором информационной системы персональных данных или сотрудником, ответственным за информационную безопасность Администрации, устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

− устанавливать программное обеспечение, указанное в Перечне запрещенного программного обеспечения (приложение 1 к настоящей Форме);

− использовать для хранения персональных данных неучтенные носители информации;

− подключать к рабочей станции и информационной системе Администрации носители информации, мобильные устройства и другое оборудование, необходимость подключения которых не относится к выполнению должностных (договорных) обязанностей.

- отключать (блокировать) средства защиты информации.

3. Администрация оставляет за собой право производить контроль использования сотрудником информационных ресурсов Администрации, а также использования технических средств обработки, хранения и передачи информации, предоставленных Администрацией.

4. Любой ущерб, вызванный нарушением конфиденциальности информации, либо однократное нарушение режима обработки конфиденциальной информации влечет дисциплинарную, гражданско-правовую, административную либо уголовную ответственность, предусмотренную действующим законодательством Российской Федерации и локальными нормативными актами Администрации.