УТВЕРЖДАЮ
Директор ГБУ СО ЯО
Краснoперекопский
психоневрологический
интернат

М.В.Филиппова
«10» 01 2020 г.

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат

1.Ответственность за выявление инцидентов информационной безопасности и реагирование на них в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат (далее – учреждение) возлагается на ответственного за обеспечение безопасности персональных данных.в информационных системах персональных данных (далее – ИСПДн).

2. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных имеет полномочия инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

3. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных обязан вести журнал учёта инцидентов информационной безопасности (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). К ним относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

4.В журнале в свободной форме описывается инцидент с указанием следующих данных:

– даты и времени;

– причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;

– информации о последствиях;

– информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам персональных данных и юридические последствия для учреждения и т.п.).

5.Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

6.В случае возникновения рецидива со стороны пользователя информационных систем персональных данных по ходатайству ответственного за организацию обработки персональных данных руководителем учреждения накладывается дисциплинарное взыскание.

7.Сокрытие нарушений и инцидентов информационной безопасности, вызванных любыми должностными лицами учреждения, является грубым нарушением трудовой дисциплины.

8.Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

– замена прикладного оборудования (мышь, клавиатура, принтер, монитор);

– установка дополнительного ПО;

– изменение сетевых настроек рабочего места;

– замена, изменение любой аппаратной части рабочего места.