Утверждаю
Директор ГБУ СО ЯО
Красноперекопский
психоневрологический интернат

_____ М.В. Филиппова
«__»_____01_____20_20_____ г.

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности в государственном бюджетном учреждении социального обслуживания Ярославской области Красноперекопский психоневрологический интернат

I. Общие положения

1.1. Настоящее Положение по работе с инцидентами информационной безопасности в государственном бюджетном учреждении социального обслуживания Ярославской области Красноперекопский психоневрологический интернат (далее - Положение) разработан в целях выявления наиболее актуальных угроз информационной безопасности, определения порядка действий пользователей информационных систем в государственном бюджетном учреждении социального обслуживания Ярославской области Красноперекопский психоневрологический интернат (далее – учреждение).

1.2.Положение разработано в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.3. Инцидент информационной безопасности – одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования

информационной системы и (или) к возникновению угроз безопасности, в том числе при обработке персональных данных.

1.4. Инциденты информационной безопасности могут быть преднамеренными или случайными и могут вызываться как техническими, так и физическими средствами. Их последствиями могут быть такие события, как несанкционированное изменение информации, ее уничтожение или другие события, которые сделают информацию недоступной.

1.5. К инцидентам информационной безопасности относятся:

- разглашение информации ограниченного распространения, не составляющей государственную тайну (далее – защищаемая информация);
- передача защищаемой информации по открытым каналам связи;
- обработка защищаемой информации на незащищенных технических средствах обработки информации;
- опубликование защищаемой информации в средствах массовой информации;
- передача носителя защищаемой информации лицу, не имеющему права доступа к ней;
- утрата или хищение носителя с защищаемой информацией;
- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой информации;
- несанкционированный доступ к информационным системам комитета;
- использование закладочных устройств и программных закладок;
- применение программных вирусов;
- неконтролируемые изменения в информационной системе;
- нарушение функционирования технических средств обработки информации, в том числе дефекты, сбои, отказы, аварии технических средств;
- дефекты, сбои, отказы в работе программного обеспечения.

1.6. В случае возникновения инцидентов информационной безопасности, порядок действий при которых не регламентирован настоящим Положением, в учреждении вырабатывается конкретный план действий с учетом текущей ситуации.

1.7. Работа с инцидентами информационной безопасности включает в себя следующие направления:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификация и регистрация инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационных системах пользователями и администраторами;
- анализ инцидентов, в том числе определение источников и причин

возникновения инцидентов, а так же оценка их последствий;

- принятие мер по устранению последствий инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

II. Ответственные за выявление инцидентов информационной безопасности и реагирование на них

2.1. В информационных системах комитета ответственными за выявление инцидентов информационной безопасности являются:

- работники Учреждения, имеющие право доступа к информационной системе;
- руководитель подразделения Учреждения, в котором выявлен инцидент;
- работник, ответственный за защиту персональных данных.

2.2. Ответственными за реагирование на инциденты в информационной системе являются:

- работники Учреждения, имеющие право доступа к информационной системе;
- руководитель подразделения Учреждения, в котором выявлен инцидент;
- работник Учреждения, ответственный за организацию обработки персональных данных, в случае, если информационная система является информационной системой персональных данных.

2.3. Вне информационной системы ответственными за выявление инцидентов являются все работники Учреждения.

2.4.Ответственными за реагирование на инциденты вне информационной системы являются:

- работник Учреждения, обнаруживший инцидент;
- руководитель подразделения, в котором выявлен инцидент;
- работник Учреждения, ответственный за организацию обработки персональных данных комитета, в случае, если существует угроза безопасности персональных данных.

III. Порядок действий при возникновении инцидентов информационной безопасности

3.1. Работа по обнаружению инцидентов информационной безопасности включает в себя мероприятия, направленные на выявление инцидентов в области информационной безопасности с помощью технических средств, в ходе контрольных мероприятий, с помощью работников Учреждения.

3.2. Работник Учреждения (пользователь), обнаруживший инцидент в

информационной системе, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, работнику Учреждения, ответственному за организацию обработки персональных данных (в случае, если информационная система является информационной системой персональных данных).

3.3. Ответственный за организацию обработки персональных данных осуществляет регистрацию инцидентов в журнале учета нештатных ситуаций Учреждения и принимает незамедлительные меры к идентификации источника инцидента информационной безопасности, восстановлению работоспособности информационной системы и устранению дестабилизирующих факторов (Приложение 1).

3.4. Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение ведение и хранение журнала – работник, ответственный за организацию обработки персональных данных в учреждении.

3.5. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценку их последствий осуществляет работник, ответственный за организацию обработки персональных данных в учреждении.

3.6. Меры по устранению последствий инцидентов включают в себя мероприятия, направленные на определение границ инцидента и ущерба от реализации угроз информационной безопасности, а также на ликвидацию последствий инцидента и полное, либо частичное возмещение ущерба.

3.7. Оценка последствий инцидента производится на основании потенциально возможного ущерба.

3.8. Планирование и принятие мер по предотвращению повторного возникновения инцидентов информационной безопасности основывается на проведении мероприятий по обучению работников Учреждения правилам и способам работы со средствами защиты информационных систем, доведении до работников Учреждения норм и требований федерального и регионального законодательства Российской Федерации, нормативных правовых актов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности, своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности, своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

IV.Заключительные положения

4.1. Настоящее Положение вступает в силу с момента его утверждения.

4.2. Изменения в Положение вносятся в случае изменения нормативных правовых актов в сфере персональных данных.

Приложение1

Государственное бюджетное учреждение социального обслуживания Ярославской области
Красноперекопский психоневрологический интернат

Журнал
регистрации инцидентов информационной безопасности

Журнал начат_____

Журнал завершен_____

Регистрация инцидентов информационной безопасности

№ п/п	ФИО, должность, структурное подразделение лица, обнаружившего инцидент	Дата выявления инцидента	Описание инцидента	Принятые меры по устранению последствий инцидента	Причины возникновения инцидента	Размер потенциально-возможного ущерба	Размер фактического ущерба	Принятые меры по предотвращению повторного возникновения инцидента