В этих целях администрация Учреждения имеет право:

- назначать ответственного за обеспечение информационной безопасности;

- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- включать требования по обеспечению информационной безопасности в коллективный договор;

- включать требования по защите информации в договоры по всем видам деятельности;

- разрабатывать перечень сведений конфиденциального характера;

- требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.

6.К организационным и функциональным документам по обеспечению информационной безопасности относятся:

- приказ о назначении ответственного за обеспечение информационной безопасности;

- соглашении между Учреждением и сотрудниками о неразглашении персональных данных воспитанников, их родителей (законных представителей), работников Учреждения;

- локальный акт, определяющий порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Учреждения.

7.Порядок допуска сотрудников Учреждения к информации:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства Российской Федерации и Учреждения об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

- контроль работника, ответственного за информационную безопасность, при работе с информацией конфиденциального характера.

8.Первоочередные мероприятия по информационной безопасности:

- защита интеллектуальной собственности Учреждения;

- защита компьютеров, локальных сетей и сети подключения к системе «Интернет» в кабинетах Учреждения;

- организация защиты конфиденциальной информации, в т.ч. персональных данных работников и воспитанников Учреждения;

- учет всех носителей конфиденциальной информации.