**Приложение № 19.**

**Инструкция IT отдела по обеспечению информационной безопасности Организации**

**Общие положения**

1. Настоящая инструкция определяет порядок действий сотрудников IT отдела по обеспечению информационной безопасности в организации.
2. Инструкция разработана с целью предотвращения несанкционированного доступа к информационным ресурсам, обеспечения целостности, доступности и конфиденциальности обрабатываемых данных.

**Основные обязанности**

1. IT отдел обеспечивает установку, настройку и техническую поддержку оборудования и программного обеспечения, используемых в информационной системе организации согласно Положению по информационной безопасности.
2. Сотрудники отдела проводят регулярные обновления системы безопасности, включая установку патчей и обновлений безопасности для защиты от известных уязвимостей
3. IT отдел осуществляет мониторинг сетевой активности на предмет обнаружения подозрительного трафика и внедряет меры для предотвращения кибератак.
4. Пункты 1.-3. Проводится при взаимодействию с отделом по информационной безопасности ( привлеченной фирмы по защите информационной безопасности).

**Процедуры управления доступом**

1. Отдел контролирует выдачу и управление учетными записями и паролями, обеспечивая их соответствие политике безопасности организации.
2. Разрабатывает и поддерживает процедуры аутентификации и авторизации для обеспечения контролируемого доступа к ресурсам.

**Ответственность за реагирование на инциденты**

1. IT отдел незамедлительно реагирует на инциденты безопасности, координирует процесс устранения последствий инцидентов и восстановления систем после атак.
2. Отдел поддерживает в актуальном состоянии планы реагирования на инциденты и обеспечивает их исполнение.

**Обучение и повышение квалификации**

1. IT отдел проводит регулярное обучение своих сотрудников по вопросам информационной безопасности и актуальным угрозам.
2. Организует обучающие сессии и семинары для пользователей информационных систем организации для повышения их осведомленности о правилах безопасного использования информационных ресурсов.