ИНФОРМАЦИОННО-КАЧЕСТВЕННАЯ БЕЗОПАСНОСТЬ ПОЛИТИКА СИСТЕМЫ УПРАВЛЕНИЯ BGYS.PLT.00

Как высшее руководство компании **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ**;

В **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ** Услуги; ISO / IEC 27001: 2017 Управление информационной безопасностью

Основная тема систем, созданных в стандарте ISMS, - продемонстрировать, что управление информационной безопасностью обеспечивается в рамках человеческих ресурсов, инфраструктуры, программного и аппаратного обеспечения, информации о клиентах, информации организации, всех бизнесов и транзакций, информации третьих лиц и финансовых ресурсов, обеспечить управление качеством и рисками, измерить результативность процессов управления информационно-качественной безопасностью и регулировать отношения с третьими лицами по вопросам, связанным с качеством информационной безопасности и удовлетворенностью клиентов.

В этом направлении целью нашей Политики ИСУБ является:

- Защита информационных активов **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ** от всех видов угроз, которые могут возникнуть изнутри или извне, осознанно или неосознанно, обеспечение доступности информации в соответствии с требованиями бизнес-процессов, выполнение требований правового законодательства, работа в направлении постоянного улучшения,
- обеспечить преемственность трех основных элементов системы управления информационной безопасностью во всех осуществляемых видах деятельности.

Конфиденциальность: Предотвращение несанкционированного доступа к конфиденциальной информации,

Целостность: Демонстрация того, что обеспечивается точность и целостность информации,

Доступность: Демонстрация того, что уполномоченные лица могут получить доступ к информации в случае необходимости,

Лидерство и приверженность: Высшее руководство компании руководит созданием и внедрением СУИБ и обеспечивает высокий уровень участия в практике СУИБ.

- Заботиться о безопасности не только данных, хранящихся в электронном виде, но и всех данных на письменных, печатных, устных и аналогичных носителях.
- Повышение осведомленности путем проведения тренингов по управлению информационной безопасностью для всего персонала.
- Сообщать команде ISMS обо всех уязвимостях в системе информационной безопасности, которые реально существуют или вызывают подозрения, и обеспечивать их расследование командой ISMS.
- Подготовка, сопровождение и тестирование планов обеспечения непрерывности бизнеса.
- Выявление существующих рисков путем проведения периодических оценок информационной безопасности. По результатам оценок рассматривать планы действий и следить за их выполнением.

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

❖ Предотвращение споров и конфликтов интересов, которые могут возникнуть в связи с заключением договоров.

❖ Она отвечает требованиям бизнеса к доступности информации и информационным системам.

Мы стремимся к этому.

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР