Политика Безопасности

ISKRATEL

Политика безопасности представляет собой рамки, объединяющие знания и практический опыт в области физической безопасности и безопасности коммуникаций. Таким образом, компания внедрила такую систему защиты, которая предотвращает злоупотребления, несанкционированные вторжения и присвоение коммерческих и других секретов.

Мы отдаем себе отчет в том, что гармоничная и хорошо организованная система безопасности требует информированности, обучения и мотивации сотрудников, тщательно отобранного программного обеспечения и оборудования, а также документированных процедур, которые включают в себя механизмы контроля.

Наша система основана на выявлении угроз, постоянном повышении уровня информированности сотрудников о возможных злоупотреблениях и интеграции самых современных механизмов безопасности в области физической, системной и программной безопасности. Правила системы безопасности доведены до сведения всех сотрудников и субподрядчиков, с подписанием обязательств о неразглашении и подчинением обязательствам компании в сфере безопасности.

Цели реализации политики безопасности

- Защита данных и информации (личной и деловой) различными способами, обеспечивающими непрерывность бизнеса и минимизирующими деловые риски.
- Предотвращение незаконного присвоения или раскрытия соответствующей коммерческой информации посторонним физическим и юридическим лицам.
- Соблюдение правил, которые применяются к работникам в процессах работы компании при обработке конфиденциальных данных и информации.
- Управление контентом и информационными инструментами, а также документацией с точки зрения уровней конфиденциальности, целостности и доступности.
- Предоставление ресурсов (ответственных лиц и инфраструктуры) для управления, эффективного функционирования и совершенствования системы, а также мониторинга и отчетности о функционировании системы.
- Принятие мер по предотвращению причинения материального или морального ущерба компании или частному лицу из-за незнания, злоупотребления или поверхностного исполнения обязанностей, а также наказание лиц, виновных в выявленных случаях.
- Снижение выявленных рисков для выполнения целей по безопасности и бизнес-целей компании.
- Руководство функционированием бизнес-процессов в соответствии с законодательной базой (Закон о защите секретной информации, Закон о защите персональных данных, Закон о защите документальных и архивных материалов, Постановление АКОС - Безопасность сетей и услуг и целостность сетей, а также Директива ЕС 2009/140 / ЕС).

Утверждено:

Željko Puljić
CEO

Документ выпущен компанией

ISKRATEL

Iskratel, d. o. o., Kranj

Ljubljanska cesta 24a
SI 4000 Kranj, Slovenia

T +386 4 207 20 00
F +386 4 207 27 12

info@iskratel.si
www.iskratel.com