

Luminor

Luminor Bank  
Информационная  
Безопасность



# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Luminor признает и понимает свою ответственность за обеспечение безопасности любой информации, доверенной нам клиентом, поставщиком или любой другой заинтересованной стороной. Неспособность обеспечить безопасность данной информации может потенциально нанести ущерб правам физических лиц, негативно повлиять на клиентов Luminor, а также привести к санкциям, штрафам и другим формам обязательств несущих за собой убытки и негативное влияние на репутацию и бренд Luminor.

Luminor очень серьезно относится к информационной безопасности, поэтому минимизация связанных с безопасностью рисков – это приоритет для нас. В связи с этим, в Luminor была принята и установлена Политика Информационной Безопасности (Information Security Policy). Данный документ закладывает основу для управления информационной безопасностью и рисками связанными с информационной безопасностью в рамках Luminor, а также обеспечивает такие требования информационной безопасности как конфиденциальность, целостность и доступность данных.

Структура Управления Информационной Безопасностью или Information Security Management Framework (ISMF) основана на международном стандарте ISO 27002 и передовых практиках. ISMF предоставляет основу для управления всеми инструментами и средствами контроля, которые банк использует для защиты своей информации. Главный Офис Управления Информационной Безопасностью или Chief Information Security Office (CISO) отвечает за руководство и координацию разработки ISMF.

Внедряя ISMF, Luminor гарантирует:

- Поддержку и разработку Политики Информационной Безопасности и Стандарта Информационной Безопасности.
- Неотъемлемую роль руководства в установлении конкретных, измеримых, достижимых, актуальных и своевременных целей, которые подлежат пересмотру и проверке через запланированные промежутки времени.
- Возложение ответственности за информационную безопасность на квалифицированных сотрудников с необходимым опытом.
- Выявление, рассмотрение и элиминация рисков связанных с информационной безопасностью в соответствии со степенью критичности данных рисков и в рамках обозначенного приемлемого риска.
- Доступность и обязательность учебных материалов об информационной безопасности для всех сотрудников.
- Внедрение средств контроля информационной безопасности, их постоянное улучшение и оценка эффективности.
- Своевременное выявление и реагирование на инциденты связанные с информационной безопасностью.
- Контроль и достижение соблюдения нормативных, законодательных, договорных и внутренних обязательств.