ვამტკიცებ:

_____
გენერალური მენეჯერი
შპს „ბათუმის ნავთობტერმინალი“
ამანდიკ კულტუმიევ
«_____» _____ 20____ წ.

УТВЕРЖДАЮ:

_____
Генеральный менеджер
ООО «Батумский Нефтяной Терминал»
Амандык Култумиев
«_____» _____ 20____ г.

მენეჯმენტის ინტეგრირებული სისტემა

პოლიტიკები და სახელმძღვანელოები

შპს «ბათუმის ნავთობტერმინალის» პოლიტიკა საინფორაციო უსაფრთხოების უზრუნველყოფის სფეროში

№ Q1-10-10-006 რევიზია 1.

ИНТЕГРИРОВАННАЯ СИСТЕМА МЕНЕДЖМЕНТА

Политики и руководства

Политика ООО «Батумский нефтяной терминал» в области обеспечения информационной безопасности

№ Q1-10-10-006 Ревизия 1.

შეთანხმებულია / СОГЛАСОВАНО:

გენერალური მენეჯერის მოადგილე ეკონომიკისა და ფინანსურ საკითხებში Заместитель генерального менеджера по экономике и финансам	/……/	არმან ხამიტბეკოვ Арман Хамитбеков
იურიდიული განყოფილების უფროსი Начальник юридического отдела	/……/	ედუარდ სააკიან Эдуард Саакян
კადრების, შრომის ანაზღაურებისა და პერსონალის მომზადების განყოფილების უფროსი Начальник отдела кадров, оплаты труда и подготовки персонала	/……/	ირინა კეპულაძე Ирина Кепуладзе
ეკოლოგიის, საწარმოო უსაფრთხოებისა და ჯანდაცვის განყოფილების უფროსი Начальник отдела экологии, производственной безопасности и здравоохранения	/……/	თენგიზ გორდელაძე Тенгиз Горделадзе
ადმინისტრაციული დირექტორი Административный директор	/……/	მზია გეგენავა Мзия Гегенава
ტექნიკური დირექტორი Технический директор	/……/	გოჩა ცირეკიძე Гоча Цирекидзе
საოპერაციო დირექტორი Операционный директор	/……/	ნინა გოგოტიშვილი Нина Гоготишвили
შესყიდვების და კონტრაქტების განყოფილების უფროსი Начальник отдела закупок и контрактов	/……/	ელდოს სატიბეკოვ Елдос Сатыбеков
საინფორმაციო ტექნოლოგიების გნაყოფილების უფროსი Начальник отдела информационных технологий	/……/	ზაზა დიდმანიძე Заза Дидманидзе
ხარისხის მართვის განყოფილების უფროსი Начальник отдела управления качеством	/……/	ლალი ქობულაძე Лали Кобуладзе

ЛИСТ РЕГИСТРАЦИЙ ИЗМЕНЕНИЙ К ДОКУМЕНТУ					
Рев.	Описание ревизии, стр.	Причина пересмотра	Должность	Подпись	Дата рев.
1	Первое издание		Начальник отдела управления качеством		**17-06-2015**

Оглавление

1. Введение:

Настоящая Политика в области обеспечения информационной безопасности устанавливает цель, задачи и основные принципы в области обеспечения информационной безопасности, которыми ООО «Батумский нефтяной терминал» (далее – Общество) руководствуется своей деятельности в сфере сохранности операционной и финансовой информации в корпоративной электронной программе Pelogas Terminal и на бумажных носителях при приеме, хранении и погрузки сырой нефти, нефтепродуктов и сжиженного углеводородного газа.

Основной целью обеспечения информационной безопасности является защита информационных систем и активов Батумского нефтяного терминала от воздействия угроз (рисков).

Настоящий документ разработан на основании требований пункта 5.2 стандарта ISO 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2. Цель:

Целью Общества в области обеспечения информационной безопасности является защита конфиденциальной информации, информационных технологий и систем Общества от возможного нанесения материального, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, носители, процессы обработки и передачи данных.

Указанная цель достигается посредством управления рисками информационной безопасности для обеспечения непрерывности основных бизнес-процессов Общества и поддержанием следующих свойств информации:

a) Конфиденциальности;
b) Целостности;
c) Доступности информации.

Успешное достижение цели настоящей Политики возможно при выполнении требований внутренних документов, регламентирующих процессы системы управления информационной безопасностью.

3. Задачи в области обеспечения информационной безопасности

Для достижения цели Общества в области обеспечения информационной безопасности решаются следующие задачи:

3.1 Ежегодное проведение внутренних аудитов информационной безопасности для своевременного выявления, предупреждения и нейтрализации угроз информационной безопасности;

3.2 Оценка рисков информационной безопасности с целью:

a) Анализа и прогнозирования источников угроз и уязвимостей информационной безопасности;

b) Установления причин и условий возникновения угроз и уязвимостей информационной безопасности;

c) Анализа влияния угроз и уязвимостей информационной безопасности на финансовое положение Общества и его репутацию.

3.3 Принятие исчерпывающих мер для бесперебойного функционирования информационных систем Общества;

3.4 Постоянное повышение осведомленности работников Общества в области информационной безопасности;

3.5 Предоставления доступа к информации только тем лицам, которым он необходим для выполнения должностных или договорных обязательств в минимально возможном объеме;

3.6 Определение владельца для каждого информационного ресурса, отвечающего за предоставления к нему доступа и эффективное функционирование мер защиты информации;

3.7 Оперативное реагирование на угрозы (риски) информационной безопасности;

3.8 Минимизация и локализация ущерба, нанесенного неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

3.9 Защиты информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и предаче по каналам связи;

3.10 Непрерывное улучшение системы управления информационной безопасностью.

4. Основные принципы в области обеспечения информационной безопасности

Обеспечение информационной безопасности и функционирование системы управления информационной безопасностью в Обществе осуществляется в соответствии со следующими основными принципами:

a) Законности;
b) Системности;
c) Комплексности;
d) Непрерывности;
e) Экономической целесообразности;
f) Персональной ответственности;
g) Гибкости системы защиты;
h) Открытости;
i) Простоты применения защитных мер и средств.

5. Термины и определения

5.1 **Риск:**
Комбинация вероятности события и его последствий.

5.2 **Политика:**
Общее намерение и направление, официально выраженная руководством.

5.3 **Угроза:**
возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации.

6. Нормативные ссылки

6.1 **ISO/IEC 27001:2013**
Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

6.2 **ISO/IEC 27002:2013**
Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации

7. Ответственности и полномочия

7.1 **Высшее руководство, руководители подразделений** несут ответственность за личное соблюдение и обеспечение соблюдения требований данной Политики в подчиненных подразделениях.

7.2 **Каждый работник** несет персональную ответственность за соблюдение требований и процедур, описанных в настоящем документе.