ПОЛИТИКА
в области охраны и безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ ПОЛИТИКИ В ОБЛАСТИ ОХРАНЫ И БЕЗОПАСНОСТИ.

Компания АО «ИНФОТЕК-БАЛТИКА М» (далее – Компания) вводит политику в области охраны и безопасности (далее – Политика), для обеспечения охраны и безопасности Компании, сотрудников, имущества и причастных лиц.

2. ЦЕЛИ И ЗАДАЧИ ПОЛИТИКИ В ОБЛАСТИ ОХРАНЫ И БЕЗОПАСНОСТИ.

Целью Политики является обеспечение координации действий всех сотрудников Компании по устранению или минимизации внутренних и внешних угроз, отмеченных в областях Политики.

Основной задачей Политики является создание системы постоянного мониторинга и учета всех возможных опасностей, нештатных ситуаций и обеспечения безопасности Компании, а так же локализация и устранение выявленных недостатков.

3. ПРОВЕРКА СИСТЕМЫ БЕЗОПАСНОСТИ И ОХРАНЫ.

Системой обеспечения охраны и безопасности руководит Ответственный за безопасность Компании. Компания использует письменные процедуры, требующие документированных периодических проверок, для выявления нарушений в области безопасности. Система безопасности оформляется в протоколах проверок безопасности, а также отчетах о нештатных ситуациях и отчетах об устранении опасностей.

Система безопасности и охраны обеспечивает определение мер реагирования на угрозы безопасности и опасные инциденты, при нарушении системы защиты, что регламентируется в отчетах и планах действий в опасных ситуациях.

4. ОБЛАСТИ ОХРАНЫ И БЕЗОПАСНОСТИ

Система обеспечения охраны и безопасности направлена на следующие области:

a) Управление доступом к рабочим местам.
b) Физическая охрана сотрудников офиса.
c) Охранная сигнализация.
d) Видеонаблюдение.
e) Антитеррористическая безопасность.
f) Экономическая безопасность.
g) Кибер безопасность.

5. ОПИСАНИЕ ОБЛАСТЕЙ ОХРАНЫ И БЕЗОПАСНОСТИ

a) Управление доступом к рабочим местам

Управление доступом к рабочим местам осуществляется посредством создания системы контроля входа-выхода на территорию Компании, с использованием электронных опознавательных карт. Данная система обеспечивает идентификацию посетителей Компании и

ограничивает доступ к закрытым зонам Компании, лицам не обладающим правами доступа.

b) **Физическая охрана сотрудников офиса.**

Физическая охрана сотрудников офиса обеспечивается за счет выявления угроз и обеспечения безопасности, с возможностью привлечения сторонних структур безопасности.

c) Охранная сигнализация

Безопасность Компании обеспечивает система сигнализации, звукового информационного уведомления сотрудников об опасности, в том числе пожарная сигнализация с динамиками оповещения.

Компания уведомляет сотрудников и руководство об уровнях опасности. Существует система обмена информацией с местными/национальными правоохранительными органами посредством телефонной и электронной связи.

d) Видеонаблюдение

В компании установлены средства видеонаблюдения для фиксации и предупреждения опасных ситуаций, обеспечения надлежащего уровня безопасности, сохранности имущества Компании и личного имущества сотрудников компании.

e) Антитеррористическая безопасность

В компании проводятся процедуры по подготовке персонала к предотвращению террористических угроз. Проводятся учения по эвакуации и инструктаж сотрудников Компании, о действиях в опасных ситуациях.

f) Экономическая безопасность

В компании проводятся процедуры по обеспечению экономической безопасности. Они включают в себя: документальную проверку контрагентов, борьбу с коррупцией и взяточничеством (включая конфликты интересов, мошенничество, отмывание денег), исполнение антикоррупционной политикой и соответствующих ей нормативных документов.

g) Кибер безопасность

В компании проводятся процедуры по обеспечению кибер безопасности.

Компания ведет реестр технических устройств и программ, содержащих конфиденциальные данные компании, в том числе устройств за пределами офиса Компании: ноутбуки, мобильные телефоны, камеры, программное обеспечение.

В компании проводится профилактическое обслуживание технических устройств, использующихся для обработки и передачи информации, о чем ведутся соответствующие записи. Техническое обслуживание проводится в соответствии с рекомендованными поставщиками интервалами обслуживания, описанными в спецификациях к устройствам и программам.

Компания использует процедуры защиты данных, и взаимодействует для этого с экспертами в области и информационной безопасности.

6. НОРМАТИВНАЯ БАЗА ПОЛИТИКИ

Настоящая Политика разработана в соответствии с законодательством Российской Федерации, нормативными документами Компании и распространяется на все структурные подразделения Компании.

По вопросам обеспечения охраны и безопасности Компания руководствуется рекомендациями CEFIC изложенными в руководстве «Код безопасности ответственной заботы» (Responsible Care Security Code)

http://www.cefic.org/Documents/IndustrySupport/RC%20tools%20for%20SMEs/Document%20Tool%20Box/Responsible%20Care%20Security%20Code%20-%20Guidance.pdf?epslanguage=en