Политика информационной безопасности

1. Назначение

Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы менеджмента информационной безопасности (СМИБ) Департамента облачных сервисов (далее - ДОС) , определяющим приоритеты, принципы и методы обеспечения информационной безопасности, в условиях наличия угроз, характерных и существенных для инфраструктуры облачных сервисов ДОС.

Требования настоящей Политики и других внутренних документов в части обеспечения информационной безопасности обязательны для исполнения всеми сотрудниками подразделений входящих в область действия СМИБ.

2. Общие положения

Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами, а также стабильное функционирование сервисов для клиентов.

Политика информационной безопасности разработана в соответствии с положениями международного стандарта ISO/IEC 27001:2013.

3. Гарантии и задачи СМИБ

3.1. Гарантии и задачи ИБ

Для обеспечения информационной безопасности предоставляемых облачных сервисов клиентам, таких как:

- аренда программных продуктов по модели подписки;
- аренда вычислительных мощностей по модели подписки;

- проектирование, разработка и инсталляция облачных инфраструктур;
- техническая поддержка в рамках облачных сервисов,

руководство гарантирует:

- повышение качества предоставляемых сервисов;
- минимизацию возможных убытков от нарушений конфиденциальности, целостности и доступности информации;
- улучшение имиджа компании на рынке.

Для соблюдения гарантий в области обеспечения ИБ ИОС системы руководство поставило задачу постоянного совершенствования системы менеджмента информационной безопасности, а именно:

- предотвращение инцидентов ИБ;
- оценка и снижение рисков от инцидентов ИБ до приемлемого уровня;
- выявление и оперативное реагирование на потенциальные угрозы ИБ и уязвимости объектов защиты;
- оперативное реагирование на изменение требований регуляторов и законов Российской Федерации.

3.2. Обязательства высшего руководства

Настоящим руководство обязуется:

- внедрение и непрерывное улучшение СИБ будет обеспечиваться достаточными ресурсами для достижения указанных в данной Политике гарантий;
- соответствовать всем выявленным требованиям;
- требовать от всех сотрудников и поставщиков соблюдения требований по информационной безопасности в соответствии с установленными политиками и процедурами.

4. Порядок пересмотра и внесения изменений.

Пересмотр положений настоящей Политики осуществляется на регулярной основе, но не реже одного раза в три года.