СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «АЛЬТЕРНАТИВНАЯ ГЕНЕРИРУЮЩАЯ КОМПАНИЯ-1»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. СВЕДЕНИЯ О ДОКУМЕНТЕ

1.1 Настоящий документ определяет Политику информационной безопасности ООО «АГК-1».

1.2 Документ разработан Отделом информационной безопасности Общества.

1.3 Срок действия: до замены (отмены).

1.4 Оригинал документа хранится в Отделе информационной безопасности.

1.5 Подразделение Общества, ответственное за документ (разработка, пересмотр, оценка), – Отдел информационной безопасности.

1.6 Настоящий документ пересматривается 1 раз в 3 года или в случае существенных изменений. Целями пересмотра документа являются:

- обеспечение постоянной пригодности/применимости документа;
- обеспечение соответствия положений документа в ответ на изменения в деятельности Общества, применяемых информационных технологиях, законодательстве в области информационной безопасности;
- обеспечение результативности применения положений документа.

При пересмотре документа необходимо оценивать возможность улучшения его положений.

1.7 Требования настоящего документа обязательны для выполнения всеми работниками Общества.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем документе применяются термины и сокращения, указанные в ISO/IEC 27000, а также следующие:

Наименование	Значение	Принятое сокращение
Общество, Организация	Общество с ограниченной ответственностью «Альтернативная генерирующая компания-1»	ООО «АГК-1»

3. НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ

ISO/IEC 27001:2013. Информационные технологии – Методы защиты - Системы менеджмента информационной безопасности – Требования.

4. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Общие положения

4.1.1 Настоящий документ определяет высокоуровневые цели и задачи обеспечения информационной безопасности Общества. Соблюдение настоящей Политики является элементом корпоративной этики.

4.1.2 Политика разработана с учетом:

– положений международного стандарта ISO/IEC 27001;

– требований законодательства Российской Федерации в области информационной безопасности;

– накопленного опыта в области обеспечения информационной безопасности;

– целей деятельности Общества, особенностей бизнес-процессов и направлений развития Общества;

– существующих и прогнозируемых угроз и рисков информационной безопасности.

4.1.3 Настоящая Политика является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности информации в Обществе;

– принятия управленческих решений и разработке практических мер по воплощению Политики и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

– координации деятельности структурных подразделений Общества при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;

– разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации.

4.1.4 Все владельцы информационных активов Общества обязаны обеспечить их защиту в соответствии с требованиями данного документа.

4.2 Цели, задачи и принципы в области информационной безопасности

4.2.1 Цели в области информационной безопасности формируются с

учетом действующих требований в области информационной безопасности, результатов оценки и обработки рисков.

4.2.2 Основными целями в области обеспечения информационной безопасности Общества являются:

– обеспечение безопасности активов Общества;

– минимизация возможных последствий от реализации угроз и рисков информационной безопасности;

– обеспечение соответствия требованиям (п. 4.7);

– обеспечение соответствия договорным обязательствам;

– обеспечение уверенности руководства Общества и заинтересованных сторон в том, что активам Общества обеспечена достаточная безопасность и защита от возможного вреда.

4.2.3 Достижение указанных целей в области информационной безопасности осуществляется путем:

– реализации, эксплуатации и совершенствования системы информационной безопасности, включающей в себя комплекс организационных, технических и правовых мер информационной безопасности;

– реализации, эксплуатации и совершенствования системы управления информационной безопасностью (п. 4.6).

4.2.4 Основными задачами обеспечения информационной безопасности являются:

– реализация комплекса мер информационной безопасности (п. 4.5), сформулированных для каждой из областей обеспечения информационной безопасности (п. 4.3);

– отслеживание, анализ и улучшение реализованного комплекса мер информационной безопасности.

4.2.5 Основными принципами обеспечения информационной безопасности являются:

– принцип экономической эффективности. Результаты от реализации мер информационной безопасности должны превышать совокупные затраты на них;

– принцип наименьших привилегий. Пользователю должны предоставляться права доступа к активам Общества с наименьшими привилегиями, необходимыми для выполнения обязанностей;

– принцип разделения полномочий. Распределение ролей и полномочий должно быть реализовано таким образом, чтобы один работник не мог нарушить критически важный для Общества процесс или создать угрозы безопасности;

– принцип эшелонированной защиты. Комплекс мер защиты должен быть реализован на различных уровнях (организационный, технический, правовой).

Безопасность, обеспечиваемая только техническими средствами, носит ограниченный характер;

– принцип невозможности обойти принятые меры защиты. Любые способы доступа к активам Общества должны быть обеспечены соответствующими мерами защиты, доступ к активам в обход принятых мер защиты должен быть исключен;

– принцип усиления самого слабого звена. Слабое звено рассматривается как самое уязвимое, самым слабым звеном может быть, как программное или аппаратное средство, так и работник Общества.

4.3 Области обеспечения информационной безопасности

К основным областям обеспечения информационной безопасности, необходимым для достижения указанных целей относятся:

- определение и классификация активов, подлежащих защите;
- управление доступом к активам;
- защита от вредоносного кода;
- оценка рисков информационной безопасности;
- управление инцидентами информационной безопасности;
- управление уязвимостями;
- мобильные устройства и удаленный доступ;
- безопасное использование ресурсов сети Интернет;
- резервное копирование;
- защита персональных данных;
- передача информационных активов третьим лицам;
- повышение осведомленности в области информационной безопасности.

4.4 Требования к обеспечению информационной безопасности

4.4.1 Для каждой из областей информационной безопасности (п. 4.3), определяются соответствующие требования к обеспечению информационной безопасности.

4.4.2 Основными источниками для задания требований к обеспечению информационной безопасности являются:

– оценка рисков информационной безопасности с учетом общей бизнес-стратегии и целей Общества. Посредством такой оценки рисков выявляются угрозы активам, определяются уязвимости и вероятности их использования,

оценивается потенциальное воздействие;

– законодательные, нормативные и контрактные требования, которые Общество и контрагенты должны выполнять;

– цели деятельности Общества, для достижения которых осуществляется работа с активами.

4.4.3 Ресурсы Общества, необходимые для реализации требований к обеспечению информационной безопасности, должны соответствовать тому потенциальному ущербу, который может возникнуть из-за отсутствия таких мер.

4.4.4 Применяемые меры безопасности, должны быть рассчитаны на предотвращение максимального потенциального ущерба.

4.4.5 Результаты оценки рисков информационной безопасности должны учитываться при определении приоритетов в реализации мер безопасности.

4.5 Меры обеспечения информационной безопасности

На основе сформированных требований к обеспечению информационной безопасности (п. 4.4) выбираются конкретные организационные, технические и правовые меры защиты, которые подлежат реализации, включая политики, процедуры, организационные меры, а также программное и аппаратное обеспечение, средства защиты соответствующего назначения.

4.6 Система управления информационной безопасностью

4.6.1 Система управления информационной безопасностью направлена на сохранение конфиденциальности, целостности, доступности информации за счет выполнения процессов управления рисками и обеспечивает уверенность в том, что риски управляются надлежащим образом.

4.6.2 Система управления информационной безопасностью составляет часть процессов Общества и встроена в общую структуру управления, и, таким образом, вопросы информационной безопасности учитываются при разработке процессов, информационных систем и средств управления.

4.6.3 Система управления информационной безопасностью должна непрерывно совершенствоваться и меняться в соответствии с потребностями Общества.

4.7 Соответствие требованиям

4.7.1 Общество ставит своей целью получение и поддержание сертификации по требованиям международного стандарта ISO/IEC 27001:2013.

4.7.2 Требования информационной безопасности должны соответствовать бизнес-целям Общества.

4.7.3 Должно быть обеспечено выполнение договорных обязательств Общества в отношении информационной безопасности, включая:

- защиту информации, составляющей коммерческую тайну,
- защиту персональных данных,
- защиту информации конфиденциального характера,

и иной информации ограниченного распространения, передаваемой на основании «Соглашений о конфиденциальности», заключаемых между Обществом и внешними сторонами.

4.7.4 Должно быть обеспечено соответствие законодательным и нормативным требованиям действующего законодательства.

4.7.5 В рамках взаимодействия Общества с компаниями, зарегистрированными на территории ЕС (вне зависимости от того, обрабатываются ли персональные данные на территории ЕС или нет), Общество ставит своей целью соблюдение требований Генерального регламента о защите персональных данных (General Data Protection Regulation, GDPR).

4.8 Ответственность

4.8.1 Отдел информационной безопасности Общества отвечает за надлежащую организацию и осуществление общего контроля исполнения требований настоящей Политики.

4.8.2 Работники Общества несут ответственность за нарушение требований настоящей Политики в соответствии с положениями действующего законодательства Российской Федерации.