



## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАРКЕТИНГОВОГО АГЕНТСТВА «WIKI INTELLECT»

Настоящая политика определяет цели и принципы обеспечения информационной безопасности в маркетинговом агентстве «WIKI INTELLECT».

1. Политика информационной безопасности маркетингового агентства «WIKI INTELLECT» разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлении Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. Политика распространяется на главный офис Компании, все филиалы, интернет-сайт маркетингового агентства «WIKI INTELLECT», имеющего доменное имя <https://wiki-intellect.ru>
3. Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с информацией, принадлежащей маркетинговому агентству «WIKI INTELLECT».
4. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность - в случае внесения в данные исключительно авторизованных изменений, доступность - при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.
5. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации и корпоративной культуры маркетингового агентства «WIKI INTELLECT» (далее – Агентство).
6. Информация является важным активом Агентства, ее защита является обязанностью каждого её сотрудника.
7. Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
8. Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.
9. Сотрудники Агентства проходят регулярное обучение в области информационной безопасности.
10. Система управления информационной безопасностью в Агентстве строится на основе международных стандартов ISO 27001 и ISO 27002.
11. Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.
12. Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Агентства и её бизнес-процессах.

13. При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Агентства и ее репутацию на рынке.
14. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.
15. Успешное достижение целей настоящей политики возможно только при выполнении положений следующих детальных политик информационной безопасности:
  - 15.1. Политика использования паролей;
  - 15.2. Политика использования сети Интернет;
  - 15.3. Политика использования электронной почты;
  - 15.4. Политика использования интернет-сайта;
  - 15.5. Политика использования страниц Агентства в социальных сетях и мессенджерах.
  - 15.6. Политика использования мобильной связи;
  - 15.7. Политики информационной безопасности платежей клиентов Агентства.
16. Несоблюдение политики информационной безопасности сотрудниками Агентства может повлечь дисциплинарные меры взыскания, иные меры, предусмотренные действующим законодательством РФ.