Положение
об информационной безопасности в дивизионе независимых компаний, осуществляющих деятельность в сферах рекламы и маркетинговых коммуникаций Игроник (далее - Игроник)

1. Общие положения

1.1 Положение об информационной безопасности (далее - Политика) определяет принципы работы с информацией, документами, системами и файлами в Игроник.
1.2 Основной целью, настоящей Политики, является защита информационных ресурсов от возможного нанесения Игроник материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носителей, процессов обработки и передачи.
1.3 Политика является документом первого уровня и обязательна к ознакомлению сотрудниками Игроник. Данное положение дополнено документами второго уровня (регламенты, инструкции, порядки, уточнения) и может быть проверено с помощью документов третьего уровня (отчёты, результаты обследования, информирование).

2. Объекты защиты

2.1 Вся информация в Игроник группируется и делится на три уровня доступа, каждый из уровней требует отдельного подхода к защите информации:
2.1.1 Общедоступная информация – информация, которая хранится на личных устройствах и используется для работы в Игроник.
2.1.2 Конфиденциальная информация – определятся положением о конфиденциальной информации.
2.1.3 Информация с ограниченным доступом – предоставляет конкурентное преимущество для бизнеса Игроник.
2.2 Защите подлежит информация, которая хранится и передаётся следующими способами:
2.2.1 В электронном виде;
2.2.2 На бумажных носителях;
2.2.3 Передаваемая устно.

3. Безопасность персонала

Роли и обязанности по обеспечению безопасности информации, описанные в соответствии с Политикой, должны быть доведены до сотрудника при трудоустройстве и внесены дирекцией по персоналу в его должностные обязанности. В данные обязанности должны входить как общие задачи по реализации и поддержке Политики, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

4. Работа с информацией

Устройства, системы, документы и файлы должны находиться под защитой на постоянной основе. Защита может быть снята только на время работы с информацией. Под снятием защиты подразумевается получение доступа к информации.
4.1 Информация, с которой производится работа в электронном виде защищается парой логин и пароль, которые применяются для доступа к:

- Компьютеру;
- Смартфону;
- Информационной системе;

- Файловому хранилищу;
- Иному ресурсу.

При работе с отдельными видами информации, а именно с информацией ограниченного доступа применяются усиленные меры защиты. К таким мерам относятся:

- Работа в отдельном помещении;
- Работа на выделенном устройстве с включенным шифрованием;
- Работа на отдельном носителе информации (флеш-карта, внешний диск, онлайн ресурс).

4.2 Информация, с которой ведётся работа в бумажном виде защищается путем контроля доступности данных документов. Особое внимание необходимо обращать материалам, которые:

- Направлены на печать;
- Находятся на рабочем месте;
- Расположены в системах хранения на рабочих местах и в общедоступных зонах.

В случаях, если информация является конфиденциальной или ограниченного доступа, то применяются дополнительные меры защиты, которые устанавливаются владельцем информации.

4.3 При работе с информацией в устном виде необходимо уточнить её уровень доступности у владельца информации и не распространять информацию внутри Игроник.

4.4 Для формирования публичной позиции необходимо использовать следующий алгоритм:

4.4.1 Получить согласование от руководства Игроник на данное действие через PR-подразделение Игроник.

4.4.2 Согласовать с PR-подразделением информацию и формат её подачи. Без согласования сотрудника PR-подразделения в письменном виде (электронном или на бумаге) не давать комментарии и не оставлять заметки или мнения от лица Игроник, включая комментарии в социальных сетях и сообщениях, которые используют атрибутику или домен *igronik.ru/com или подобные.

4.5 При получении информации, которая является конфиденциальной или ограниченного доступа, необходимо определить дополнительные меры по её защите с владельцем информации.

5. Контроль доступа

5.1 В Игроник не применяется политика безответственности или перекладывания ответственности на руководителя или владельцев бизнеса.

5.2 Допуск в офисы, офисы и склады компаний, которые предоставляют услуги хранения, и другие объекты Игроник ограничен. Допуск на объекты предоставляются по установленным процедурам.

5.3 Допуск к информации защищается логином и паролем, а также дополнительными средствами защиты, которые устанавливаются отдельными инструкциями.

5.4 У любой информации, данных, документов или систем в Игроник существует единственный владелец. Единственным владельцем информации является представитель Игроник, который её создал или инициировал создание:

- Владельцы бизнеса;
- Директора или руководители;
- Руководители проекта/задачи;
- Сотрудник/создатель информации/данных/файла;
- Подрядчик (самозанятые, индивидуальные предприниматели и др.).

5.5 Все ключи доступа (как физические, так и электронные) передаются при устройстве на работу или проведению работ с Игроник в качестве партнёра или подрядчика. После

окончания работ с Игроник ключи доступа подлежат сдаче или уничтожению /отключению дирекцией технологий (далее - ДТ).

5.6 Информация без владельца подлежит уничтожению. За уничтожение информации в электронном виде отвечает ДТ. За уничтожение информации на бумажных носителях отвечает административная дирекция.

5.7 Запрещено передавать/предоставлять доступ к ключам доступа (ключи от прохода в помещения, пароли, ключи электронных цифровых подписей и прочее).

6. Допустимые ресурсы

В Игроник допускается к использованию ресурсы, которые необходимы для реализации основной цели (коммерческой деятельности). Набор и перечень инструментов в обязательном порядке должен быть согласован с руководством ДТ Игроник.

7. Управление инцидентами

При наступлении события инцидента (утери), получения доступа сторонних лиц к конфиденциальной информации или информации ограниченного доступа, необходимо незамедлительно сообщить об этом руководству Игроник. Под руководством подразумевается непосредственный руководитель. Руководитель информирует владельцев бизнеса о факте утечки информации и предлагает план по ликвидации последствий и принятию мер по недопущению утечки в будущем.

8. Управление непрерывностью

При работе с информацией всех трёх уровней допуска с целью обеспечения непрерывности и повышения устойчивости бизнеса Игроник после каждого инцидента и утечек информации проводится подробный разбор.

9. Соблюдение законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Игроник к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии. Данная область курируется юридическим отделом Игроник.