**ДЕЛОВЫЕ ПРАВИЛА БЕЗОПАСНОГО ОБРАЩЕНИЯ С ИНФОРМАЦИЕЙ**

**Назначение: ключевые сообщения об обращении с информацией, полученной от компании Lilly или предоставленной от ее имени, в дальнейшем именуемой «Информация».**

**Почему это важно?**

- Ваша организация и ее сотрудники являются ценными помощниками компании Lilly, и действия, которые вы и ваши сотрудники предпринимаете, являются частью первой и лучшей линии защиты от компрометации Информации.
- Защита Информации важна для компании Lilly и пациентов, которым мы служим.

Чтобы и в дальнейшем снижать риски при обращении с Информацией, в текущие методы работы должны быть включены следующие ключевые сообщения, основанные на передовых отраслевых практиках.

**В целом:**

- Избегайте дублирования электронных или бумажных экземпляров документов, содержащих Информацию, за исключением случаев крайней необходимости.

**Хранение электронных данных:**

- Электронные файлы, включающие Информацию, должны храниться в безопасности. Без разрешения со стороны компании Lilly запрещается использовать съемные устройства хранения, такие как внешние жесткие диски и USB-накопители.
    - При предоставлении доступа к файлам следует использовать принцип наименьших привилегий (т. е. доступ к Информации должен предоставляться только тем, кому это необходимо, не больше, чем необходимо, и только на необходимое время). Доступ следует пересматривать соразмерно степени важности. Это включает контролируемые вами или вашими субподрядчиками места хранения.
    - Если сотрудник уходит из компании или у него больше нет служебной необходимости получать доступ к Информации, следует своевременно закрывать доступ.
- Без разрешения со стороны компании Lilly Информацию ЗАПРЕЩАЕТСЯ хранить в следующих местах:
    - Личные устройства сотрудников, такие как ноутбуки, iPad и т. д.
    - Внешние службы хранения или сайты.

**Электронная передача данных:**

- Электронные файлы, включающие Информацию, должны передаваться безопасным способом. Чтобы определить предпочтительный способ передачи Информации, проконсультируйтесь со своим контактным лицом в компании Lilly. Без разрешения со стороны компании Lilly запрещается использовать съемные устройства хранения, такие как внешние жесткие диски, компакт-диски, DVD-диски и USB-накопители.
- ЗАПРЕЩАЕТСЯ передача информации с использованием следующих средств:
    - Незащищенная электронная почта (если это не является допустимым в соответствии с уровнем важности).
    - Внешние устройства хранения, такие как внешний жесткий диск или USB-накопитель (без разрешения со стороны компании Lilly).
    - Личная электронная почта.

**Телеконференции и онлайн-встречи:**

- Для планирования и проведения встреч по вопросам бизнеса используйте одобренные компанией Lilly службы конференций. Если у вас есть вопросы, связанные с телеконференциями и онлайн-встречами, проконсультируйтесь со своим контактным лицом в компании Lilly.
- Учитывайте свое окружение и будьте осторожны при обсуждении Информации.

**Физическая безопасность:**

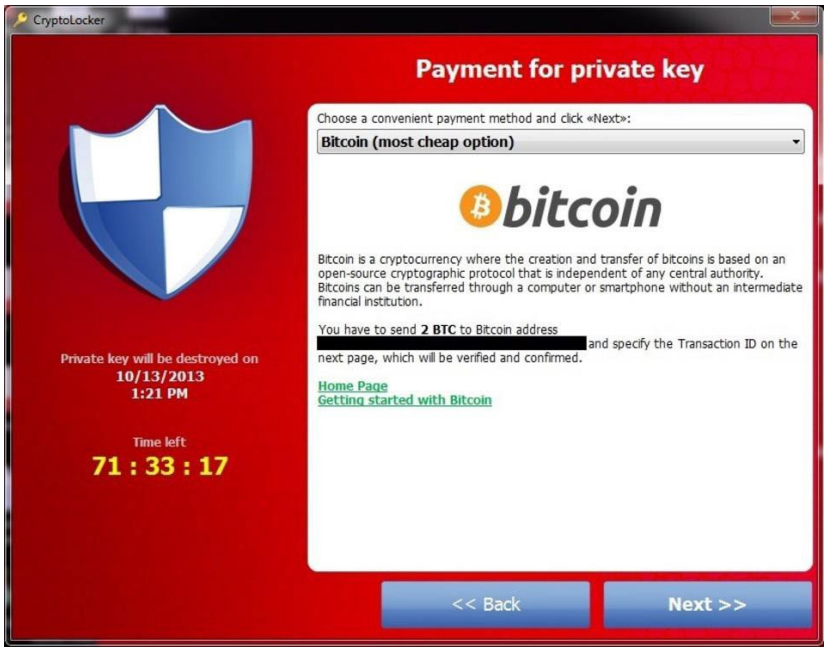
- Поддерживайте свое рабочее пространство в безопасности:
  - Блокируйте доступ к своим устройствам КАЖДЫЙ раз, когда вы отходите от них.
  - Если вы отлучаетесь на день, уезжаете в командировку или в отпуск, устройства следует помещать в запираемый шкаф, использовать трос с замком или брать с собой.
  - Если вы отлучаетесь на день, уезжаете в командировку или в отпуск, запирайте свой стол, шкафы и ячейку или офис.
  - Не оставляйте бумажные документы на принтерах.
  - Уничтожайте Информацию с соблюдением конфиденциальности (например, в устройствах измельчения, или «шредерах»).

**Мгновенные сообщения и SMS:**

- Для обмена мгновенными сообщениями и SMS в служебных целях используйте одобренный компанией Lilly инструмент. Если у вас есть вопросы, связанные с обменом мгновенными сообщениями или SMS, проконсультируйтесь со своим контактным лицом в компании Lilly.

**Сообщение о происшествиях, связанных с информационной безопасностью:**

- Своевременно сообщайте о происшествиях своему контактному лицу в компании Lilly. Происшествия включают, помимо прочего, следующее:
  - Сообщение электронной почты с Информацией было случайно отправлено не тому получателю.
  - Были утеряны или украдены ноутбук, жесткий диск или съемное запоминающее устройство, содержащие Информацию.
  - Субподрядчик с доступом к Информации предупреждает вашу компанию о происшествии.
  - Была получена программа-вымогатель — вредоносная программа, созданная для блокировки доступа к устройству до выплаты указанной суммы. См. пример ниже. Немедленное выполнение следующих действий может помочь снизить риск:
    - Отсоедините сетевой кабель или выключите беспроводной адаптер.
    - Переведите устройство в спящий режим.



**Остерегайтесь социальной инженерии** *(например, фишинга, вишинга, SMS-фишинга)***!**

- Социальная инженерия — это использование обмана для манипулирования людьми, чтобы они разгласили конфиденциальную или личную информацию, которая может использоваться в мошеннических целях. Мошенники маскируются под авторитетный источник, пытаясь украсть личные данные или получить Информацию, такую как пароли, банковские реквизиты, номера кредитных карт и т. д.
    - **Фишинг** (электронная почта)
        - Попытка фишинга — это неожиданное сообщение, отличающееся следующими особенностями:
            - Тревожный призыв к действию (например, задержка платежа по вашей кредитной карте).
            - Элемент времени (например, что-то подлежит оплате в течение двух дней).
            - Последствия (например, решите эту проблему, или с вами случится что-то нехорошее).
            - Грамматические ошибки или опечатки в словах.
            - И всегда имеется элемент, который предлагается нажать, например ссылка или вложение.
        - Если вы нажмете неизвестное вложение или ссылку в сообщении электронной почты, ваш компьютер и вся сеть могут быть скомпрометированы.

    - **Вишинг** (телефонные звонки или голосовые сообщения)
        - Попытка вишинга (голосового фишинга) — это неожиданный телефонный звонок, который:
            - Требует подтверждения Информации или запрашивает Информацию.
            - Может использоваться в сочетании с фишинг-атакой.
    - **SMS-фишинг** (текстовые сообщения SMS)
        - Попытка SMS-фишинга — это неожиданное SMS-сообщение, которое:
            - Требует подтверждения Информации или запрашивает Информацию.
            - Может использоваться в сочетании с фишинг-атакой.
            - Как правило, содержит элемент для выбора, например ссылку или вложение.

- **Если у вас есть адрес электронной почты компании Lilly**, вы примете участие в официальной программе обучения Lilly по фишингу.
    - О сотрудниках, которые повторно нажимают элементы фишинговых сообщений, будет сообщаться третьей стороне с предполагаемым дополнительным обучением. Если у вас есть вопросы, связанные с официальной программой обучения Lilly по фишингу, проконсультируйтесь со своим контактным лицом в компании Lilly.
    - Если вы используете учетную запись электронной почты Lilly o365, сообщайте о подозрительных сообщениях электронной почты с помощью кнопки «Report Phishing» (Сообщить о фишинге) на ленте Outlook «Home» (Главная).


    - Если вы подключены к внутренней сети Lilly через VPN или virtual.lilly.com, сообщайте о подозрительных сообщениях с помощью формы cyber@lilly.com.

- **Остановитесь и подумайте. Используйте свою интуицию:**
    - Если сообщение электронной почты кажется подозрительным, внимательно рассмотрите на него.
    - Не нажимайте ссылки и не открывайте вложения, если вы их не ожидали.
    - Если у вас нет адреса электронной почты компании Lilly и вы нажали ссылку или открыли вложение в сообщении, которое считаете подозрительным, сообщите об этом, используя процесс вашего работодателя.

**Если у вас есть вопросы или опасения:**

- По вопросам или опасениям, связанным с любым из вышеуказанных пунктов, проконсультируйтесь со своим контактным лицом компании Lilly.
- Эта информация также доступна на портале для поставщиков Supplier Portal под заголовком «Operating Responsibility» (Ответственная работа) раздела «Supplier Resources» (Ресурсы для поставщиков).