?????????? ?????? ? ????????????? ?? ?????

- ПРОЦЕДУРА РАБОТЫ С ПОСТАВЩИКАМИ ИТ УСЛУГ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

????????? ?????? ? ???????????? ?? ????? ????????? «SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Цель

2. Область Применения

3. Ответственный за применение процедуры

4. Определения

5. Выбор поставщика ит услуг

5.1. Оценка рисков аутсорсинга

5.2. Соглашения о неразглашении

6. Контракты с поставщиками ит услуг

6.1. Требования к безопасности

6.2. Соблюдение требований контракта

6.3. Соглашения об уровне обслуживания

6.4. Проверка средств контроля безопасности, используемых Поставщиком ИТ услуг

6.5. Право на аудиторскую проверку

6.6. Предварительное уведомление об изменениях

6.7. Уведомления об инцидентах информационной безопасности

6.8. Защита данных Поставщиками ИТ услуг

7. Обязанности поставщика ит услуг

7.1. Требования к безопасности

7.2. Роли и обязанности в сфере информационной безопасности

7.3. Раскрытие информации о субконтрактных услугах

7.4. Нарушения безопасности и штрафы

7.5. Право утверждения персонала для ключевых должностей

7.6. Местонахождение данных

8. Управление рисками поставщика ит услуг

8.1. Оценка риска в рамках процесса переговоров с Поставщиками ИТ услуг

8.2. Непрерывность бизнеса и аварийное восстановление

9. Защита данных университета, находящихся у поставщиков ит услуг

9.1. Извлечение данных / уничтожение ресурсов Университета

9.2. Передача информации

9.3. Уведомление об инцидентах

1. ????

Настоящая Процедура работы (далее -Процедура) с Поставщиками ИТ услуг Учреждения «SDU University» (далее – Университет) разработана с целью обеспечение последовательного применения правил информационной безопасности к поставщикам и провайдерами ИТ услуг Университета. Это необходимо для защиты конфиденциальной информации Университета, обеспечивающей оптимальный баланс риска для информационной безопасности и потребности в услугах, необходимых для выполнения основных задач деловой деятельности.

2. ??????? ??????????

Настоящая Процедура в области информационной безопасности охватывает процедуры, контракты и соглашения, затрагивающие следующие элементы:

- Деятельность, осуществляемая Поставщикам ИТ услуг от имени Университета;
- Информационные системы, принадлежащие Университету, но контролируемые Поставщикам ИТ услуг;
- Информационные системы, содержащие данные Университета, но принадлежащие и контролируемые Поставщикам ИТ услуг.

3. ????????????? ?? ?????????? ?????????

Ответственным за надлежащее применение и соблюдение Процедуры является Заведующий Отдела информационно-технической поддержки.

4. ???????????

Конфиденциальная информация – критичная информация, которая в случае разглашения неавторизованным лицам может нанести значительный ущерб Университету. Информация с таким уровнем классификации должна быть наиболее защищена от несанкционированного доступа или модификации.

Поставщик ИТ услуг - это любая внешняя организация, с которой Университет имеет действующие договорные отношения. Средства контроля, представленные в настоящей Процедуре, охватывают все этапы отношений с данным поставщиком ИТ услуг от его выбора до окончания контракта. Поставщиком ИТ услуг также может называться:

- независимый поставщик и/или провайдер ИТ услуг
- производитель (разработчик)
- консультант

5. ????? ?????????? ?? ?????

5.1. ?????? ?????? ???????????

Перед началом процесса заключения контрактов с любым Поставщиком ИТ услуг необходимо провести оценку рисков для определения последствий безопасности при аутсорсинге и допустимость идентифицированных рисков.

5.2. ?????????? ? ?????????????

Перед получением доступа к любой конфиденциальной информации Поставщики ИТ услуг должны подписать соответствующее соглашение о неразглашении.

6. ????????? ? ???????????? ?? ?????

6.1. ?????????? ? ????????????

По возможности, контракты между Университетом и Поставщиками ИТ услуг должны содержать требования к информационной безопасности. Эти требования должны отражать тип услуг, предоставляемых данными Поставщиками ИТ услуг, устранение соответствующих рисков для безопасности коммерческих тайн, прав на объекты интеллектуальной собственности и конфиденциальной информации Университета.

6.2. ?????????? ?????????? ?????????

В договорах должно быть указано, что среды Поставщика ИТ услуг должны соответствовать или превосходить требования в области информационной безопасности Университета.

6.3. ?????????? ?? ?????? ????????????

Во всех контрактах, которые включают соглашения об уровне обслуживания (SLA) для предоставляемых услуг должны быть четко прописаны объем работ и порядок действий, гарантируемые показатели качества услуг, а также нарушение гарантируемых в SLA показателей.

6.4. ???????? ??????? ???????? ????????????, ???????????? ??????????? ?? ?????

При необходимости и до заключения контракта, Университет должен проводить проверку деятельности Поставщика ИТ услуг для подтверждения того, что осуществляемая деятельность соответствует политике безопасности Университета и требованиям контракта. Объем и форма такой оценки должны выявлять риски безопасности для Университета в случае нарушений, допущенных Поставщиком ИТ услуг.

6.5. ????? ?? ??????????? ????????

Во всех контрактах с Поставщиком ИТ услуг должно указываться, что Университет сохраняет за собой право на проведение аудита Поставщика ИТ услуг либо самостоятельно, либо с привлечением утвержденной независимой стороны.

6.6. ?????????????? ??????????? ?? ??????????

Во всех контрактах с Поставщиком ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должно указываться, что Поставщик ИТ услуг уведомляет за 5 дней о всех существенных изменениях в деловой и технической среде Поставщика ИТ услуг до вступления их в силу.

6.7. *??????????? ?? ?????????? ????????????? ???????????*

Во всех контрактах с Поставщиком ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должно указываться, что Поставщик ИТ услуг должен незамедлительно уведомить Университет о любых инцидентах информационной безопасности, которые могут оказать влияние на услуги, оказываемые Университет, либо информации Университета, которая находится под контролем Поставщика ИТ услуг.

6.8. *?????? ?????? ???????????? ?? ?????*

Контракты между Университетом и Поставщиками ИТ услуг должны указывать, что данные Университета, находящиеся в технической среде Поставщика ИТ услуг, должны быть логически или физически отделены от данных других клиентов и всегда должны быть зашифрованы.

7. *??????????? ?????????? ?? ?????*

7.1. ?????????? ? ????????????

В контрактах между Университетом и Поставщиками ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должно быть указано, что Поставщик ИТ услуг обязан поддерживать информацию Университета и системы на уровне безопасности, который соответствует, или превышает уровень

определенный в начале первого квартала фискального года. (Пункт 9.1 настоящей Процедуры)

7.2. ???? ? ??????????? ? ????? ????????????? ???????????

Контракты между Университетом и Поставщиками ИТ услуг должны четко указывать за какие действия связанные с информационной безопасностью несут ответственность Поставщики ИТ услуг, а за какие Университет.

7.3. ????????? ?????????? ? ????????????? ???????

Контракты между Университетом и Поставщиками ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должны указывать, что Поставщик ИТ услуг, до оказания услуг, должен раскрыть, была ли передана субподрядчику какая-либо часть контрактных услуг, предоставляемых Университету, и что такие субподрядчики обязаны соблюдать те же требования информационной безопасности, что и Поставщик ИТ услуг, и что Поставщик ИТ услуг несет ответственность за обеспечение соблюдения субподрядчиками договорных обязательств.

7.4. ????????? ???????????? ? ??????

Контракты между Университетом и Поставщиками ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должны содержать формулировку, в которой прямо указано право расторгнуть договор в одностороннем порядке, если по усмотрению Университета может быть доказано, что Поставщик ИТ услуг не соблюдает условия контракта, включая, выполнение требований безопасности Университета. Несоблюдение требований информационной безопасности является нарушением условий договора и облагается штрафом.

7.5. ????? ??????????? ????????? ??? ???????? ??????????

Контракты между Университетом и Поставщиками ИТ услуг оставляют право за Университетом одобрять или отклонять персонал, который выполняет обязанности на территории Университета или обрабатывает данные,

классифицированные как конфиденциальные или персональные.

7.6. ?????????????? ??????

Контракты между Университетом и Поставщиками ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета должны четко указывать в каких юрисдикциях будут находиться, обрабатываться и использоваться данные Университета. В случае изменение этих юрисдикций в течение срока действия контракта Поставщик ИТ услуг обязан заранее уведомить Университет.

8. ?????????? ??????? ?????????? ?? ?????

8.1. ?????? ????? ? ?????? ???????? ??????????? ? ???????????? ?? ?????

В рамках процесса переговоров по контракту проводится оценка безопасности всех Поставщиков ИТ услуг, которые хранят или обрабатывают конфиденциальную информацию, либо разрабатывают или управляют информационной системой Университета для проверки, того что Поставщики ИТ услуг соответствуют или превосходят требованиям процедур, стандартов Университета, а также законодательных и нормативных актов в области информационной безопасности. Данная проверка должна хранится на протяжении срока действия контракта с Поставщиком ИТ услуг.

8.2. ????????????? ??????? ? ????????? ??????????????

Технические возможности Поставщиков ИТ услуг по непрерывности деятельности и аварийного восстановления систем (BCP / DR) должны быть проверены на соответствие требованиям Университета, а контракты, которые включают соглашения об уровне обслуживания (SLA) для предоставляемых услуг, должны содержать Целевую точку восстановления (RPO) и Целевое время восстановления (RTO).

9. ?????? ?????? ????????????, ??????????? ? ???????????? ?? ?????

9.1. ?????????? ?????? / ??????????? ???????? ????????????

Контракты, заключенные с Поставщиками ИТ услуг должны предусматривать возврат или уничтожение ресурсов, данных или информации ТФСКЗ по завершении участия или по требованию Университета.

9.2. ???????? ??????????

Электронная передача конфиденциальной информации должна осуществляться только через безопасные, одобренные механизмы, и все физические носители должны быть зашифрованы во время передачи такой информации.

9.3. ??????????? ?? ??????????

Контракты, заключенные с Поставщиками ИТ услуг, должны определять процедуру и соглашение об уровне услуг для информирования Университета об утере, краже, изменении или доступе уполномоченных лиц к данным Университета.