

План за изпълнение на изискванията по ДОРА изготвяне на необходимата документация

1. Управление на ИКТ риска

а. Политики и процедури:

Политика за управление на ИКТ риска:

- **Цел:** Дефинира целите и обхвата на управлението на ИКТ риска.
- **Съдържание:**
 - Обща цел на политиката.
 - Обхват и приложимост.
 - Основни принципи и подходи към управлението на ИКТ риска.
 - Роли и отговорности.
 - Процедури за одобрение и актуализация на политиката.

Процедури за управление на ИКТ риска:

- **Цел:** Описват конкретни стъпки и действия за идентифициране, оценка и контрол на ИКТ рисковете.
- **Съдържание:**
 - Процедури за идентификация на рисковете (включително използвани инструменти и техники).
 - Процедури за оценка на рисковете (включително методологии и критерии за оценка).
 - Контролни механизми за управление на идентифицираните рискове.
 - Процедури за мониторинг и преглед на рисковете.
 - Процедури за документиране и докладване на резултатите.

б. Системи за управление на риска:

Описание на използваните инструменти и методологии:

- **Цел:** Осигурява ясна представа за технологиите и методите, използвани за управление на ИКТ риска.
- **Съдържание:**
 - Идентификация на използваните софтуерни и хардуерни инструменти.
 - Подробности за методологиите (напр. COSO, ISO 31000, NIST).
 - Примери за прилагане на тези методологии в организацията.

Доклад за оценка на ИКТ риска:

- **Цел:** Предоставя резултатите от оценката на рисковете и идентифицираните уязвимости.
- **Съдържание:**
 - Обобщение на методологията и процеса на оценка.
 - Описание на идентифицираните рискове.
 - Оценка на вероятността и въздействието на всеки риск.
 - Препоръки за контролни мерки.

Контролни механизми за намаляване на ИКТ рисковете:

- **Цел:** Определя конкретни мерки и контроли за управление на идентифицираните рискове.
- **Съдържание:**
 - Описание на всяка контролна мярка.
 - Роли и отговорности за изпълнение на контролните мерки.
 - Процедури за мониторинг и преглед на ефективността на контролните мерки.
 - Планиране и подготовка за периодични одити и прегледи.

2. Инцидентно докладване

а. Докладване на инциденти:

Процедури за докладване на инциденти:

- **Цел:** Дефинира процеса за докладване на ИКТ инциденти.
- **Съдържание:**
 - Описание на инцидента.
 - Време и дата на възникване.
 - Засегнати системи и услуги.
 - Идентифициране на причината за инцидента.
 - Въздействие върху бизнеса (напр. загуба на данни, нарушаване на услуги).

Форма за докладване на инциденти:

- **Цел:** Стандартизира формата за докладване на инциденти.
- **Съдържание:**
 - Заглавие и описание на инцидента.
 - Дата и час на инцидента.
 - Засегнати ресурси и услуги.
 - Причина за инцидента.
 - Въздействие и оценка на щетите.
 - Предприети мерки за ограничаване и възстановяване.

Списък на всички значими ИКТ инциденти:

- **Цел:** Води регистър на всички значими ИКТ инциденти.
- **Съдържание:**
 - Дата и час на инцидента.
 - Кратко описание на инцидента.
 - Засегнати системи и услуги.
 - Въздействие и оценка на щетите.
 - Предприети мерки за възстановяване.
 - План за предотвратяване на бъдещи инциденти.

в. Анализ и уроци:

Анализ на причините за инцидентите:

- **Цел:** Идентифицира основните причини за възникване на инцидентите.
- **Съдържание:**
 - Детайлен анализ на всеки инцидент.
 - Идентифициране на слабости и уязвимости в системите.
 - Връзка между инцидентите и идентифицираните рискове.
 - Оценка на ефективността на съществуващите контроли.

Изводи и препоръки:

- **Цел:** Определя мерки за предотвратяване на бъдещи инциденти и подобряване на реакцията при възникване на инциденти.
- **Съдържание:**
 - Изводи, извлечени от анализирания инцидент.
 - Препоръки за подобряване на контролните мерки.
 - Оценка на ефективността на предприетите мерки за ограничаване.
 - Планове за обучение и повишаване на осведомеността на служителите.

3. Оперативна устойчивост

а. Планиране и възстановяване:

План за възстановяване след инциденти (Disaster Recovery Plan - DRP):

- **Цел:** Осигурява насоки и процедури за възстановяване на ИКТ системите и услугите след инцидент.
- **Съдържание:**
 - Обхват и цел на плана.
 - Идентификация на критичните системи и ресурси.
 - Процедури за възстановяване на данните и системите.
 - Отговорности и роли на екипа за възстановяване.
 - Контактни данни на ключови лица и доставчици.
 - Периодичен преглед и актуализация на плана.

План за непрекъснатост на бизнеса (Business Continuity Plan - BCP):

- **Цел:** Гарантира продължителността на бизнес процесите по време на изслед инциденти.
- **Съдържание:**
 - Описание на критичните бизнес функции и процеси.
 - Стратегии за непрекъснатост на бизнеса.
 - Процедури за поддържане на критични операции.
 - Роли и отговорности на BCP екипа.
 - Комуникационен план за информирание на всички заинтересовани страни.
 - Планове за възстановяване на нормалните операции.

b. Тестове на устойчивостта:

Резултати от тестове на оперативната устойчивост:

- **Цел:** Демонстрира ефективността на плановете за възстановяване и непрекъснатост на бизнеса.
- **Съдържание:**
 - Описание на проведените тестове и сценарии.
 - Резултати от тестовете.
 - Идентифицирани слабости и уязвимости.
 - Препоръки за подобрене.
 - Планове за корективни действия и последващи тестове.

Тестове за стрес и сценарии за извънредни ситуации:

- **Цел:** Оценка на устойчивостта на системите и процесите при екстремни условия.
- **Съдържание:**
 - Описание на различните сценарии за стрес тестове.
 - Методологии за провеждане на тестовете.
 - Анализ на резултатите и идентифициране на потенциални слабости.
 - Планове за подобрене и подготовка за бъдещи тестове.

4. Управление на трети страни

a. Доставчици на ИКТ услуги:

Регистър на доставчиците:

- **Цел:** Води регистър на всички външни доставчици на ИКТ услуги.
- **Съдържание:**
 - Име и контактна информация на доставчика.
 - Описание на предоставяните услуги.
 - Договорни условия и срокове.

- Интерактивни сесии, семинари и уебинари.
- Роли и отговорности на участниците.
- Методи за оценка на ефективността на обучението (тестове, анкети).
- График и честота на обучителните сесии.

Специализирани обучения за ИКТ персонала:

- **Цел:** Повишава квалификацията на ИКТ персонала и ги подготвя за управление на сложни ИКТ системи.
- **Съдържание:**
 - Курсове по специфични технологии и инструменти.
 - Обучение по най-добрите практики за управление на ИКТ инфраструктура.
 - Сертификационни програми (напр. CISSP, CISM).
 - Практически упражнения и симулации.
 - Оценка на знанията и уменията на участниците.

а. Повишаване на съзнателността:

Кампания за осведоменост относно ИКТ рисковете:

- **Цел:** Повишава осведомеността на всички служители за значимостта на ИКТ сигурността.
- **Съдържание:**
 - Редовни информационни бюлетини и електронни писма.
 - Постери и инфографики в офисите.
 - Вътрешни презентации и лекции.
 - Видео материали и интерактивни курсове онлайн.
 - Споделяне на реални случаи и уроци от инциденти.

Дни на сигурността и семинари:

- **Цел:** Организира събития, които да насърчат ангажираността на служителите към ИКТ сигурността.
- **Съдържание:**
 - Дни на отворени врати за ИКТ сигурност.
 - Семинари и работилници с гост-лектори.
 - Състезания и викторини за повишаване на знанията.
 - Дискусионни панели и Q&A сесии.
 - Демонстрации на нови технологии и решения.

в. Оценка и подобрение:

Процедури за оценка на ефективността на обучението и осведомеността:

- **Цел:** Оценява ефективността на програмите за обучение и осведоменост.
- **Съдържание:**
 - Анкети и въпросници за обратна връзка.
 - Оценка на знанията преди и след обученията.
 - Анализ на инциденти и случаи, за да се установи дали обучението било ефективно.
 - Доклади и препоръки за подобрения.

План за непрекъснато подобрение:

- **Цел:** Гарантира, че програмите за обучение и осведоменост се актуализират и подобряват редовно.
- **Съдържание:**
 - Анализ на резултатите от оценките и обратната връзка.
 - Идентифициране на области за подобрение.
 - Актуализация на обучителните материали и методи.
 - Планиране на нови инициативи и събития.

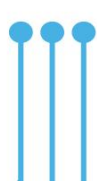
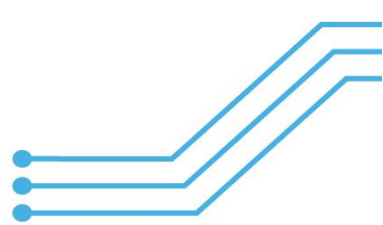
5. Съответствие със законодателството

а. Мерки за съответствие с ДОРА:

Документ за съответствие с ДОРА:

- **Цел:** Осигурява подробна документация на мерките, предприети за съответствие с Digital Operational Resilience Act (ДОРА).
- **Съдържание:**
 - Общо описание на изискванията на ДОРА.
 - Обхват и обекти на съответствие (напр. системи, процеси, роли).
 - Политики и процедури, въведени за съответствие с ДОРА.
 - Идентифицирани рискове и мерки за управление на тези рискове.
 - Процедури за мониторинг и одит на съответствието.

Регистър на регулаторните изисквания:

- **Цел:** Поддържа актуален списък на всички регулаторни изисквания, свързани с ИКТ сигурността и оперативната устойчивост.
 - **Съдържание:**
 - Идентификация на релевантни закони и регулации.
 - Описание на конкретните изисквания.
 - Дата на влизане в сила и срокове за изпълнение.
 - Отговорни лица и отдели за изпълнение на изискванията.
- 
- 

План за изпълнение на ДОРА:

- **Цел:** Определя конкретни стъпки и срокове за изпълнение на изискванията на ДОРА.
- **Съдържание:**
 - Разбивка на изискванията на ДОРА на конкретни задачи.
 - График и крайни срокове за изпълнение.
 - Разпределение на ресурси и отговорности.
 - Методи за мониторинг и оценка на напредъка.
 - Планове за управление на промяната.

в. Процедури за мониторинг на съответствието:

Процедури за вътрешни одити и прегледи:

- **Цел:** Осигурява редовен мониторинг и оценка на съответствието с ДОРА и други регулаторни изисквания.
- **Съдържание:**
 - График за провеждане на вътрешни одити и прегледи.
 - Методи за оценка на съответствието.
 - Документация на резултатите от одитите.
 - Планове за корективни действия при отклонения от съответствието.
 - Проследяване на изпълнението на корективните действия.

Процедури за външни одити и сертификации:

- **Цел:** Осигурява съответствие с ДОРА чрез външни оценки и сертификации.
- **Съдържание:**
 - Идентифициране на независими външни одитори.
 - График за външни одити и сертификации.
 - Подготовка на необходимите документи и информация за външните одити.
 - Документация на резултатите и препоръките от външните одити.
 - Планове за изпълнение на препоръките и корективни действия

с. Документиране и отчетност:

Доклад за съответствие:

- **Цел:** Предоставя обобщена информация за съответствието с ДОРА на ръководството и регулаторните органи.
- **Съдържание:**
 - Обобщение на предприетите мерки за съответствие.
 - Резултати от вътрешните и външните одити.
 - Оценка на съответствието и идентифицирани отклонения.
 - Планове за корективни действия и последващи стъпки.
 - Препоръки за подобрене и бъдещи инициативи.

Регистър на съответствието:

- **Цел:** Поддържа подробна документация на всички действия и мерки, предприети за съответствие с ДОРА.
- **Съдържание:**
 - Списък на всички предприети мерки и действия.
 - Дати на изпълнение и отговорни лица.
 - Резултати от изпълнението на мерките.
 - Документация на всички одити, прегледи и оценки.