ПОАД „ЦКБ-Сила" АД, гр. София

ПОЛИТИКА ПО СИГУРНОСТ НА ИНФОРМАЦИЯТА

Влиза в сила от: 01.04.2013 г.

Digitally signed by:George Todorov Todorov
Date:01.04.2013 18:48
Reason:I am approving this document
Location:POAD "CCB-Sila"

0. Термини и Определения

Наличност
Свойството за достъпност и използваемост на информацията при заявка от упълномощено лице

Поверителност
Свойството информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси

Цялостност
Свойството за опазване на точността и целостта на информационни активи

Сигурност на Информацията
Запазване на сигурност, цялостност и наличност на информацията

Система за Управление на Сигурността на Информацията
Онази част от общата система за управление, основана на подхода за риска, свързан с организацията, за изграждане, внедряване, функциониране, наблюдение, преглед, поддържане, и подобряване сигурността на информацията

Инцидент, свързан със сигурността на информацията
Единично събитие или поредица от нежелани и неочаквани събития, свързани със сигурността на информацията, които има голяма вероятност да навредят на дейността и да застрашат сигурността на информацията

Управление на риска
Координирани действия за насочване и контролиране на организацията по отношение на риска

Въздействие върху риска
Процес за подбор и прилагане на мерки с цел изменение на риска

Декларация за Приложимост
Документ, описващ целите по контрола и механизмите за контрол, които се отнасят и са приложими към СУСИ на организацията.

Бележка: термините са взети от ISO/IEC 27001:2005

1. Декларация на Ръководството

Ръководството на ПОАД „ЦКБ-Сила" АД, с местоположение ул. „Стефан Караджа" 2, гр. София, България е ангажирано със запазване на поверителността, цялостността и наличността на пълния набор от физически и електронни информационни активи на организацията, за да запази конкурентоспособността, паричния поток, рентабилността, правното, нормативното и договорно съответствие и търговски имидж.

Изискванията за информацията и за сигурността на информацията ще се управляват чрез изграждане, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на документирана Система за Управление на Сигурността на Информацията (СУСИ) в съответствие с изискванията на стандарта ISO 27001:2005 и стратегическите цели на Организацията.

2. Цели по сигурността на информацията

Целите по сигурността на информацията в ПОАД „ЦКБ-Сила" АД са:

- Да защити информацията на организацията от заплахи, независимо дали те са вътрешни или външни, умишлени или случайни;
- Да способства за сигурно споделяне на информация;
- Да насърчи непрекъснатото и професионално използване на информацията;
- Да гарантира, че всеки един служител е наясно с ролята си по използване и защита на информацията;
- Да гарантира непрекъсваемостта на бизнеса и минимизира вредата върху бизнеса;
- Да защити организацията от съдебна отговорност и неподходящо използване на информацията;
- Да гарантира съответствие с действащите закони, регулации и директиви.

3. Обхват на СУСИ

Обхватът на СУСИ се дефинира както е посочено:

a) Услуги
   i. Предоставяне на услуги в областта на допълнителното пенсионно осигуряване
b) Организационни единици
   i. Всички структурни звена на дружеството
c) Местоположение
   i. Централен офис - ул. „Стефан Караджа" 2, гр. София
d) Ресурси
   Използваните ресурси са описани подробно в списъка на активите.
e) Изключения
   i. Описани са в Декларация за Приложимост на дружеството

4. Стратегическо Управление на Риска

Действащият стратегически бизнес план и рамката за управление на риска на ПОАД „ЦКБ-Сила" АД дават контекста за идентифициране, преценяване, оценяване и контролиране на рисковете свързани с информацията чрез изграждане и поддържане на СУСИ. Оценката на Риска, Декларацията за Приложимост и Плана за Въздействие върху Риска определят как ще се контролират рисковете свързани с информацията. Дирекция „Информационни технологии и комуникации" е отговорна за управлението и поддържането на Плана за Въздействие върху Риска. Допълнителни оценки на риска може, при необходимост, да бъдат извършени, за да се определят подходящи механизми за контрол за специфични рискове.

5. Изисквания за Съответствие

Организацията ще спазва всички законови, нормативни и договорни задължения, които имат отношение към нейните информационни системи, като (но не само):

- Кодекс за социално осигуряване;
- Закон за защита на личните данни;
- Закон за електронния документ и електронния подпис;
- Наредба № 47 от 11.07.2012 г. за изискванията към информационните системи на пенсионноосигурителните дружества;
- Закон за счетоводството.

6. Организация на Сигурността на Информацията

ПОАД „ЦКБ-Сила" АД е създала Комисия по Сигурност на Информацията, председателствана от Изпълнителен Директор и включваща Директор Дирекция Информационни и комуникационни Технологии, Ръководител на специализирана служба Вътрешен контрол, Директор Дирекция „Финансово счетоводна" и Директор Дирекция „Информационно обслужване и анализи" за поддържане на рамката на СУСИ и периодичен преглед на политиката по сигурността.

7. Информационна Сигурност - Осъзнаване и Обучение

Ръководството на ПОАД „ЦКБ-Сила" АД, всички служители на пълно и непълно работно време, подизпълнители, консултанти по проекти и външни страни са и ще бъдат запознавани с техните отговорности (определени в техните длъжностни характеристики или договори) да пазят сигурността на информацията, да докладват за пробиви в сигурността (в съответствие с политиката и процедурите) и да действат в съгласие с изискванията на СУСИ. Последствията от нарушаване на политиката по сигурност се определят в съответствие с дисциплинарен процес, внедрен в ПОАД „ЦКБ-Сила" АД. Целият персонал ще премине обучение по сигурност на информацията, а по-специализираният персонал ще получи подходящо специализирано обучение по сигурност на информацията.

8. Непрекъсваемост на Бизнеса

ПОАД „ЦКБ-Сила" АД организира защитата на критични бизнес процеси от ефектите на големи пробиви в информационните системи или бедствия, и гарантира тяхното навременно възстановяване.

В дружеството е внедрен процес за управление на непрекъсваемостта на бизнеса, за да се минимизира въздействието върху организацията и да може тя да се възстанови от загубата на информационни активи. Идентифицирани са всички критични бизнес процеси.
Направен е анализ на въздействието на бедствия, пробиви в сигурността, загуба на услуга и неналичност на услуга върху бизнеса.

9. Преглед на Политиката по Сигурност на Информацията

Преглед на политиката по сигурност на информацията ще се извършва минимум веднъж годишно или при настъпване на значителни промени, за да се гарантира нейната надеждност, адекватност и ефективност.

10. Комуникация на политиката

Политиката по сигурност на информацията е одобрена от ръководството и е комуникирана до всички служители, доставчици и трети страни, за да се гарантира, че те разбират своите отговорности.