Allianz

Процедура за сигурност на информацията

Ангажиране на доставчици на трети страни

Приложение 1: Checklist за предварително проучване на доставчиците на услуги

Version1 / **Effective**: 12.09.2017

ЦЕЛ

Този контролен списък се използва за оценката на сигурността като част от RFI процеса за избор на трето лице, предоставящо услуги на AGCS.

Контролният лист се основава на ISO 27001: 2005 и е подравнен с номерацията и подразделите, дефинирани в стандарта ISO. За повече подробности, моля, вижте документа по ISO. Поради ограничения на лицензирането, AGCS не може да предостави копие от стандарта ISO.

Полето "Да / Не" съдържа информация само дали изискването е изпълнено или не (Да, Не или Не). Моля, обяснете "N / A" (не е приложимо) с няколко думи. Полето "Коментари" може да се използва, за да се обясни защо едно изискване е изпълнено или не. Не се изисква да се документира поверителна информация или доказателства за изпълнението.

Моля, попълнете списъка за проверка напълно. Въпросите, които не са отговорили, ще бъдат оценени с "Не".

представяне

Име на доставчика на услуги	
Заглавие на предложеното участие	
Име и заглавие на	

Информация за връзка с	
Дата на изготвяне	

Checklist

5. Политика на сигурност

Реф.№	Изискване	Да/Не	Коментари
5.1	Имате ли политика за защита на ИТ, която обхваща изискваните услуги?		

6. Организация на информационната сигурност

Реф.№	Изискване	Да/Не	Коментари
6.1	Имате ли организация за ИТ сигурност, която да определя отговорностите и процедурите?		
6.2	Ще се предоставя ли услуга, предоставена на AGCS, на външни изпълнители?		

7. Управление на активи

Реф.№	Изискване	Да/Не	Коментари
7.1	Имате ли процедури за определяне на отговорностите за обработка на активи?		
7.2	Имате ли процедури за класифициране на информацията на място?		

8. Сигурност на човешките ресурси

Реф.№	Изискване	Да/Не	Коментари
8.1	Установени ли са ролите и отговорностите на служителите, процедурата за скрининг за кандидатите за работа и условията за наемане на работа?		

8.2	Установени ли са отговорностите на ръководството по време на наемането на работа, осведомеността за сигурността и дисциплинарните процеси		
8.3	Процедурата за прекратяване на трудовия договор е определена, включваща връщане на активи и премахване на права за достъп?		

9. Физическа и екологична сигурност

Реф.№	Изискване	Да/Не	Коментари
9.1	Съответните области като сгради, офиси, помещения, съоръжения, центрове за данни и т.н. са физически защитени, напр. с огради, физически контрол на достъпа?		
9.2	Цялото оборудване е физически защитено? Това включва и мобилно оборудване извън площадката и изхвърляне на оборудване.		

10.Управление на комуникациите и операциите

Реф.№	Изискване	Да/Не	Коментари
10.1	Имате ли действащи процедури за определяне на оперативните процедури, управлението на промените, задълженията и различните среди (развитие, тестване, работа)?		
10.2	Ако ползвате услугите на трета страна (виж изискване 6.2), са ли доставката на услугата, промените в нея и нейното наблюдение?		
10.3	Имате ли въведени процедури за планиране на системата и приемане?		
10.4	Имате ли противодействие срещу злонамерен и мобилен код?		
10.5	Имате ли процедури за архивиране?		
10.6	Имате ли процедури за управление на мрежовата сигурност?		
10.7	Имате ли процедури, които да дефинират манипулирането на медиите, включително отстраняването на медиите?		

10.8	Имате ли процедури за обмен на информация, които обхващат физически медиен транзит, както и електронна комуникация?		
10.9	Имате ли процедури за покриване на използването на системи за електронна търговия, системи за онлайн транзакции и използване на обществено достъпна информация?		
10.10	Имате ли действащи процедури за определяне на мониторинга, записването и одита на дейностите в системата?		

11. Контрол на достъпа

Реф.№	Изискване	Да/Не	Коментари
11.1	Имате ли политика за определяне на контрола за достъп въз основа на бизнес цели?		
11.2	Имате ли процедури, обхващащи процеса на управление на потребителите (регистрация, управление на привилегии, управление на пароли, преглед на разрешения)?		
11.3	Имате ли процедура за дефиниране на отговорностите на потребителя относно обработката на пароли и ясни бюро / екран?		
11.4	Имате ли процедури, които ясно и изчерпателно дефинират контрола за достъп до мрежата, включително идентифициране на устройства, удостоверяване, разделяне на мрежата, контрол на връзката и управление на маршрута?		
11.5	Имате ли процедури за дефиниране на сигурността на операционната система и сигурността на приложенията (съдържащи най-малко сигурна регистрация, удостоверяване, управление на паролата и време за изчакване на сесията)?		
11.6	Имате ли процедури за определяне на ограничения за достъп и изолация на информация, може би за изключително критична информация?		
11.7	Имате ли процедури за покриване на използването на мобилни компютри и работа на разстояние?		

12. Придобиване, разработване и поддръжка на системи

Реф.№	Изискване	Да/Не	Коментари
12.1	Имате ли действащи процедури, определящи изискванията за сигурност във връзка с бизнес изискванията?		
12.2	Имате ли процедури за разработка на приложения, определящи, че всяко заявление трябва да валидира своя вход и неговата продукция, както и целостта на съобщенията и вътрешната обработка да се контролира?		
12.3	Имате ли процедури за разработване на приложения, определящи правилното използване на криптографски средства?		
12.4	Имате ли процедури, които контролират инсталирането на софтуер на операционни системи, селекцията и обработката на данните от тестовете и ограничаването на достъпа до изходния код?		
12.5	Имате ли процедури, които покриват управлението на промяната на софтуерната актуализация или промените в основната операционна система?		
12.6	Ако е приложимо (вж. Изискване 2.2), тази процедура обхваща и разработването на софтуер на външни изпълнители?		

13. Управление на инцидентите по сигурността на информацията

Реф.№	Изискване	Да/Не	Коментари
13.1	Имате ли процедура за определяне на редовно отчитане на събития и слабости в областта на сигурността?		
13.2	Имате ли процедура за дефиниране на отговорностите, реагиращите процедури в случай на инциденти, процедурите за събиране на доказателства и процедурите за обучение за инциденти?		

14. Управление на непрекъснатост на работата

Реф.№	Изискване	Да/Не	Коментари
14.1	Имате ли процедури за изграждане на цялостно управление на непрекъснатостта на бизнеса (стратегия, насоки и т.н.)?		