

# Технически изисквания

---

## Технически цели на проекта

- Внедряване на решение за класификация и защита на конфиденциална бизнес информация на базата на Microsoft Azure Information Protection;

## Технически изисквания към решението

Решението следва да отговаря на следните изисквания:

- Да се интегрира с наличната в EBH Active Directory (за автентикация и оторизация)
- Да поддържа ръчна и автоматична класификация и защита на документи, и електронна поща в Microsoft Office 2010 или по-нова версия (Word, Excel, PowerPoint, Outlook);
- Да поддържа класификация и защита на PDF документи, с възможност за преглед на документите през Adobe Reader;
- Да поддържа защита на произволни файлови формати.
- Да предоставя възможност за автоматично прилагане на политики за защита на чувствителна информация чрез Exchange 2010 или по-нова версия;
- Да е съвместим с Microsoft SharePoint 2010 или по-нова версия и да предоставя възможност за прилагане на политики за защита на информацията в отделни библиотеки от документи;
- Да се интегрира с Windows Server 2008R2 File Classification Infrastructure или по-нова версия на операционната система и да предоставя възможност за автоматична защита на документи на база на наличието на чувствителна информация или конкретна папка;
- Да предоставя възможност за откриване на чувствителна информация върху файлови сървъри и SharePoint библиотеки. Възможност за откриване на лични данни свързани с регламента GDPR.
- Да предоставя възможност за създаване на различни етикети за класификация на документи с възможност за прилагане на защита на информацията – позволения/забрана на корекция, копиране, четене, запис, печат, препращане;
- Да предоставя възможност на създателите на документи или имейли сами да определят правата за достъп и потребителите имащи право на достъп до документа. След прилагане на съответните права за достъп, те трябва да стават неразделна част от документ или имейл, независимо къде(десктоп, USB, локален сървър или интернет пространство) и как се съхранява или споделя с други потребители;
- Получаване на известия при отваряне на документ или опит за неоторизиран достъп;
- Да предоставя възможност за проследяване на опити за оторизиран или неоторизиран достъп до защитени документи в организацията или извън нея; Да предоставя възможност за проследяване и визуализация върху географска карта.

- Да предоставя възможност за задаване на дата на валидност на защитен документ и премахване на достъп след изтичане на съответния срок;
- Да предоставя възможност за премахване на достъп до вече споделен документ;
- Да бъде съвместимо с мобилни платформи, като iOS, Android и Blackberry 10;
- За целите на точното и коректно изпълнение, кандидатът трябва да гарантира, че има директен достъп до продуктите групи, разработващи съответните продукти и технологии, на собственика на софтуера, предмет на поръчката – Microsoft.

### Обхват на проекта:

- Планиране на дизайна и конфигурацията на решението в EBH;
- Подготовка на необходимата инфраструктура за внедряване на решението;
  - ADFS, Azure AD Connect, RMS Connector, AIP Scanner
  - Анализ и подготовка на Active Directory за синхронизация и федерация с Azure AD
- Създаване на политики за класификация и защита на информация;
- Интеграция на следните системи с AIP:
  - SharePoint Server;
  - Exchange Server;
  - Windows Server File Classification Infrastructure.
- Конфигуриране на AIP Scanner за откриване и класифициране на данни съхранявани на файлов сървър и SharePoint.
- Внедряване на Azure Information Protection клиент за пилотна група от потребители
- Разработка на документация:
  - Ръководство за внедряване