ПРАВИЛА И УСЛОВИЯ ЗА ПОЛЗВАНЕ И ПРЕДОСТАВЯНЕ НА ПАКЕТ КИБЕРСИГУРНОСТ

Настоящите Правила („Правилата“) съдържат специфичните условия и параметри на услугите - продуктите, включени в избраните от клиентите Пакети, предоставяни от А1 България ЕАД, ЕИК: 131468980 („Доставчика“ или А1) при условията на Договор за Пакет Киберсигурност ("Договор/ът"), Общи условия за информационно-комуникационни технологични (ICT) услуги, предоставяни от А1 БЪЛГАРИЯ ЕАД и лицензионни споразумения (заедно "Услуги/те" или „Продукти/те, поотделно "Услуга/та").
Продуктите са част от Пакета по смисъла на Договора, сключен между А1 и Клиента.

1. MANAGED NEXT GENERATION FIREWALL

1.1.1. Услугата Next Generation Firewall се предоставя като продукт – част от избрания Пакет Киберсигурност и представлява система (хардуерно устройство и софтуерни лицензии) за извършване на наблюдение на входящия и изходящия мрежови трафик, идентифициране и неутрализиране на заплахи от интернет пространството, упражняване на контрол върху трафика с налагане на правила и политики. Доставчикът предоставя първоначалната инсталация и конфигурация на доставените хардуерни устройства;
1.2. Услугата се предоставя от А1 България в качеството му на оторизиран партньор на Checkpoint в съответствие с (а) условията на Договора, приложенията, тези Правила, Общи условия за информационно-комуникационни технологични (ICT) услуги, предоставяни от А1 БЪЛГАРИЯ ЕАД и (б) Условията за ползване (EULA) на софтуера/хардуера за информационна сигурност, предварително дефинирани от производителя на софтуера/хардуера Checkpoint. EULA документите на производителя на софтуера/хардуера за информационна сигурност се намират на официалната интернет страница на Checkpoint.
1.3. Особености на услугата:
1.3.1. Клиентът не придобива право на собственост върху софтуерни лицензи и хардуерно оборудване, като същите се предоставят за ползване за срока на Договора.
1.3.2. Услугата се предоставя чрез хардуерни устройства, които се инсталират в посочена от Клиента локация. Устройствата се поддържат в рамките на гаранционните условия на производителя от технически екип на Доставчика. След първоначална инсталация и конфигурация на хардуерните устройства, инсталирани при Клиента по този Договор се поддържат хардуерно и софтуерно от страна на Доставчика, в съответствие с условия за поддръжка на производителя.
1.3.3. Допълнителни конфигурации, промени и/или настройки на Услугите се заявяват от оторизирано контактно лице от страна на Клиента по имейл или телефон.
1.3.4. Дейностите по допълнителните настройки се оценяват и заплащат допълнително от Клиента, ако времето за тяхното изпълнение надвишава включените в месечната такса за Услугата човеко-часове или се налага допълнителна разработка от страна на технически специалисти на Доставчика.
1.3.5. Ако при установено от техническите лица на Доставчика повишаване на ползваните от Клиента ресурси /капацитет в Mbps/ се налага предоставяне на ново хардуерно устройство, с различни параметри, подмяна се извършва след подписване на анекс към Договора с нови ценови условия.
1.3.6. При стартиране на Услугата се конфигурира предварително дефинирана политика за сигурност.

1.3.7. Ако Клиентът ползва негарантиран интернет /високоскоростен интернет/ от А1 България и ползва WiFi функция от устройствата, с които този интернет се предоставя /ONT рутер или DOCSYS модем/ тази интернет връзка не се покрива от NGFW устройството и няма да бъде защитена от настроените политики за сигурност. В тези случаи е необходимо WiFi функцията на тези устройства да бъде спряна и Клиентът да използва алтернативна WiFi мрежа от устройство, което се свързва към LAN порт на NGFW.
1.3.8. С оглед избягване на всякакво съмнение и независимо от това кой е доставчик на интернет достъп за Клиента, ако WiFi функцията на устройството за Интернет при инсталация на NGFW устройството след него, не бъде изключена, А1 България не носи отговорност при настъпили събития, представляващи заплаха за мрежовата и IT сигурност на клиентската инфраструктура през тази WiFi мрежа.
1.3.9. За да работи NGFW защитата ефективно е необходимо интернет достъпа, който се ползва в локацията на Клиента да се доставя след като е преминал през NGFW устройството /по фиксирана мрежа или безжична такава/. Ако, въпреки това, Клиентът продължи да ползва интернет достъп през мрежови порт на устройство, което не е монтирано зад NGFW, А1 България не носи отговорност при настъпили събития, представляващи заплаха за мрежовата и IT сигурност на клиентската инфраструктура на съответния адрес.
1.4. Включени елементи на Услугата
1) FW Storage на логовете
2) Централизирано управление от страна на специалисти на А1
3) Регулярен седмичен репорт за работата на услугата
4) Конфигурация на аларми в случай на регистрирани заплахи
5) Мониторинг
6) Защита от външни заплахи през интернет
7) Защита на вътрешната мрежа
8) Интеграция към MS Active Directory срещу допълнително заплащане
9) SSL VPN Access конфигурация
10) Поддръжка на конфигурацията за периода на договора
11) Хардуерна и софтуерна поддръжка
12) URL Filtering, Application control, SSL Decryption
13) А1 извършва инсталация, първоначална конфигурация и настройка, мониторинг и поддръжка на услугата за периода на договора
14) Поддръжка на тел. +359 88 1515 или support@a1.bg
15) Инспекция на трафика с цел разпознаване и блокиране на зловредно съдържание
16) IPS система за защита от познати уязвимости в софтуерните продукти
17) Базиран на Google Authenticator MFA, за VPNдостъпа
1.4.1. Устройствата, с които се предоставя услугата не поддържат WiFi функционалност. За клиента се избира подходящото устройство на базата на броя потребители, броя едновременни сесии и капацитета на интернет достъп на локацията, на която се инсталира устройството.
1.5. Предоставяне на услугата:
1.5.1. Предоставянето на Услугата стартира след датата на подписване на Договора и имплементация на оборудването. Имплементацията на Услугата се удостоверява с подписване на Протокол за приемане на Услугата, който се подписва от представители на ДОСТАВЧИКА и на КЛИЕНТА. С подписване на Протокола рискът от погиване на устройствата се прехвърля на Клиента.

1.5.2. За целите конфигурацията на услугата, страните попълват Въпросник, съдържащ следната информация: Обща информация; Фаза I – Обща информация за Firewall; Фаза II – Информация за внедряването на Firewall. Клиентът се задължава да предостави точна и коректна информация за попълване на Въпросника. Попълненият въпросник е неразделна част от Договора.
1.5.3. На потребителите на Клиента се предоставя двуфакторна автентикация за достъп до ресурси през VPN, който е конфигуриран чрез Managed NGFW услугата. За целта потребителите на Клиента трябва да ползват т.н. Google Authenticator, чрез който се осъществява вторият фактор на автентикация за достъп след въвеждането на потребителско име и парола.
1.5.4. За да поддържа нивото на договорените услуги, ДОСТАВЧИКЪТ си запазва правото да извършва регулярна профилактика на оборудването, съоръженията и ресурсите, чрез които се предоставя Услугата. Профилактиката се извършва от ДОСТАВЧИКА, който е длъжен предварително да уведоми КЛИЕНТА за точното време, продължителност на профилактиката и очаквания ефект от нея върху доставяните услуги и техните параметри. В установения за профилактика времеви интервал е допустимо пълно отпадане на всяка една от предоставяните за КЛИЕНТА услуги. ДОСТАВЧИКЪТ се ангажира профилактиката да се извършва в неработна част от денонощието и за минималния възможен времеви интервал.
1.5.5. За да осигури надеждност и сигурност на договорените услуги, ДОСТАВЧИКЪТ си запазва правото да извършва обновяване на софтуерните компоненти при възникване на необходимост. Обновяванията и настройките, които изискват частични или пълни прекъсвания на предоставяните услуги ще бъдат планирани, като за целта предварително ще бъде уговорен времеви интервал между КЛИЕНТА и ДОСТАВЧИКА. В установения за обновяване и надстройка времеви интервал е допустимо пълно отпадане на всяка една от предоставяните за КЛИЕНТА услуги.
1.5.6. Инсталация и конфигурация:
1) Защитните стени ще бъдат първоначално конфигурирани съгласно добрите практики в политиките за сигурност и в съответствие с попълнен Въпросник, неразделна част към Договора. Клиентът предоставя достъп на мрежовите архитекти на А1 България до съществуващите мрежови устройства с цел избягване на пропуски и проблеми при превключване към новата услуга.
2) След конфигурацията на устройствата, те ще бъдат монтирани от инженерен екип за инсталация на А1 България. Мрежови архитект на А1 България се свързва дистанционно към защитната стена, за да провери дали всички параметри са в зададената конфигурация.
3) Клиентът е длъжен да провери незабавно дали във вътрешната му мрежа всичко функционира коректно и да потвърди или предостави информация относно проявени проблеми. След приключване на дейността по инсталация и конфигурация се подписва Приемо предавателен протокол с екипа за инсталация на А1 България, който е на място.
4) За предоставяне на услугата е необходимо Клиентът да разполага и да предостави статичен реален IP адрес от доставчика на интернет.
6) Допълнителни конфигурации се заявяват от оторизирано контактно лице от страна на клиента по имейл или телефон, както е дефинирано в договора. Дейностите по допълнителните настройки се оценяват и заплащат допълнително от клиента, ако времето за тяхното изпълнение надвишава включените в месечната такса за Услугата човеко-часове или се налага допълнителна сложна разработка от страна на технически специалисти на А1.
7) Промени по вече въведените настройки се заявяват от оторизирано контактно лице от страна на клиента, посочено в договора, по имейл или телефон, както следва:

i. На емейл support@a1.bg
ii. На телефон 088 1515
h. При необходимост, клиентът има възможност на повече от 1 (един) брой интернет доставчици на един адрес.
i. Клиентът има право на достъп до логовете на NGFW устройството, които се съхраняват локално на него.

Заявените промени се изпълняват в рамките на включените на месечна база човеко-часове за управление на услугата от страна на инженери на А1 България /освен в описаните в т.4g изключения/ в рамките на до 5 работни дни от заявката.
1.5.6.1. Включени елементи за конфигурация при първоначално стартиране на услугата:
1) Първоначална конфигурация на интерфейси - WAN, Internal (LAN) интерфейси
2) DHCP
3) Static routing
4) Dynamic routing
5) NAT
6) Outbound traffic policies
7) Traffic Shaping
8) SSL VPN – за до 15 потребителя
9) URL Fiter
10) DNS Filter
11) Application Control
12) Anti-Virus
13) IPS
14) Threat Emulation
15) SSL Decryption
16) Настройка за получаване на седмичен репорт
17) Настройка на достъп до NGFW устройството
18) Upgrade - Актуализация на фърмуер до най-новата възможна стабилна версия

1.5. Задължения за Клиента:
1.5.1. При планирана промяна в ползвания от Клиента капацитет на достъп до Интернет, независимо дали през основна или резервна свързаност, същият се задължава да уведоми ДОСТАВЧИКА поне един месец /30 календарни дни/ преди влизане в сила на промяната. Ако в резултат на липсата на такова предупреждение за промяна, настъпи нарушаване на качеството на услугата или тя напълно отпадне, ДОСТАВЧИКЪТ не носи отговорност. Ако в този случай се налага подмяна на устройството с цел поемане на по-високия капацитет, се подписва Анекс към договора с нови финансови условия.
1.5.2. Клиентът е длъжен да разполага с поне един реален статичен IP адрес, който да представи на Доставчика с цел конфигуриране на Услугата. Ако Клиентът не може да предостави един реален статичен IP адрес, услугата не може да бъде предоставена, като Договорът се прекратява без да се дължат неустойки от която и да е страна.
1.5.3. При конфигурация на SSL Decryption /декриптиране на трафик и инспекция за него/ е клиентът се задължава да инсталира на крайните устройства – лаптопи и настолни компютри SSL сертификат, който ще получи по email от инженери на А1 България. Ако клиентът не инсталира този сертификат на устройствата, функцията не може да се изпълни и А1 на носи отговорност за щети, породени от липса на тази функция.

1.5.4. При конфигуриране на VPN за отдалечен достъп до ресурси във вътрешната мрежа на Клиента, Клиентът се задължава да инсталира на крайните си устройства лаптопи и настолни компютри т.н. VPN агент, който ще бъде предоставен от Инженер на А1 България. Ако Клиентът не инсталира този софтуер на устройствата, функцията не може да се изпълни и А1 не носи отговорност за щети породени от липса на тази функция.
1.6. Клиентът има възможност да заявява проблеми или желание за пренастройки, като добавяне или премахване на достъп до определени сайтове, добавяне и премахване на мрежи, както и други промени свързани със защитните стени и комутаторите. Всички заявки за администриране на устройствата се изпращане на имейл на support@a1.bg или се подават на телефон 088 1515. Услугите са ограничени до броя часове работа на мрежови администратор, които са включени на месец в зависимост от избрания пакет за услугата. Ако е необходимо повече време, то се заплаща допълнително, както е дефинирано в Договора. При необходимост от сериозни промени се работи на проектен принцип, където се изготвя отделна оферта.

2. Endpoint Protection – Sentinel One

2.1. Услугата Endpoint Protection предоставя като продукт – част от избрания Пакет Киберсигурност и представлява защита на крайни устройства на Клиента от кибер заплахи, включително и откриване и отстраняване на зловреден софтуер.
2.2. Услугата се предоставя от А1 БЪЛГАРИЯ ЕАД в качеството му на оторизиран партньор на SentinelOne, Inc. (SentinelOne) в съответствие с (а) условията на Договора, приложенията, тези Правила, Общи условия за информационно-комуникационни технологични (ICT) услуги, предоставяни от А1 БЪЛГАРИЯ ЕАД , Общите условия на А1 за Дигитални услуги, Декларацията за защита на данните от А1 България ЕАД за А1 Market Place и (б) Условията на SentinelOne.
2.3. Услугата се предоставя чрез софтуерни агенти, представляващи софтуерни програми, генерирани на базата на заплатен лиценз, които се инсталират на устройствата на Клиента и са валидни за конкретен тип операционна система.
2.4. Обхват на услугата:
2.4.1. Правото на ползване на софтуерни лицензи за Endpoint Protection SentinelOne (Софтуера);
2.4.2. Първоначална конфигурация на услугата;
2.4.3. Софтуерна актуализация и техническа поддръжка на лицензите;
2.4.4. Предоставяне на услугата по модел „as a service".
2.4.5. Софтуерните функционалности на Endpoint Protection пакет Complete:

Категория	Функционалност
Endpoint Protection	Static AI /Статичен анализ с използване на Изкуствен интелект/
	Behavioral AI /Поведенчески анализ с използване на Изкуствен интелект/
	Анализ на документи /откриване на заплахи в тях/, прикачени файлове, файлове, свалени от интернет
	Fileless, Exploits /идентифициране и анализ на злонамерени действия по използване на съществуващи уязвимости в софтуера при клиента – атаки, които не произтичат от заразени файлове/

	Откриване и защита срещу 0-day атаки, онлайн и офлайн /информацията за атаката се съдържа в агента, инсталиран на устройството/
	Идентифициране и анализ на отклоненията от стандартно поведение на ползвателя.
	Управление на инвентара – цялостна информация за устройствата в мрежата и софтуера на тях
Response - Отговор	Remediation and Roll Back – Саниране на устройството и връщането му в състояние от преди атаката, бърза и лесна възможност за възстановяване на криптирани или изтрити от вируси файлове.
	Network Quarantine – налагане на изолация на заразеното устройство от мрежата, така, че да не може да зарази цялата мрежа
	Full Remote Shell – Пълен отдалечен достъп до наблюдаваните устройства
	Device Control /USB, Bluetooth/ - Управление на устройството, контрол над използването на USB, Bluetooth.
	Firewall Control – Управление на защитната стена на устройството
	Vulnerability Management – Отриване и управление на уязвимостите в софтуера, с който работят устройствата
EDR/Threat Hunting	Attack Storyline – Проследява се пълната история на атаката с конкретната причина за нея
	Deep Visibility /Including Encrypted traffic/ - Видимост на атаките дори в криптиран трафик

2.5. Услугата се ползва при следните условия:
2.5.1. А1 създава профил на Клиента в уеб-базирана платформата за управление на Услугата - А1 Market Place (Платформата). В него Доставчикът алокира заявените по реда на съответните приложения лицензи. А1 предоставя на Клиента достъп до софтуерен агент, който трябва да се инсталира на устройствата на Клиента, които ще бъдат защитени (Устройствата).
2.5.2. Услугата не се предоставя за MAC устройства. Софтуерните агенти трябва да се свалят на устройствата и да се инсталират на тях, за което отговорност носи Клиентът или негов представител. С предоставяне на достъпа, софтуерните продукти се считат за активни и стартира ползването на Услугата. Инструкцията за инсталиране на продукта се предоставяна Клиента. Като първоначална настройка на Услугата, А1 активира стандартна политика за защита.
2.5.3. При необходимост от Solution Design се изготвя и предоставя отделен проект, включващ финансови условия. При одобрение на проекта, страните подписват допълнително споразумение към договора.
2.6.. За да осигури надеждност и сигурност на услугите, А1 си запазва правото да извършва обновяване на софтуерните компоненти при възникване на необходимост. Обновяванията и надстройките, които изискват частични или пълни прекъсвания на предоставяните услуги ще бъдат планирани, като за целта предварително ще бъде уговорен времеви интервал между Клиента и А1. В установения за обновяване и надстройка времеви интервал е допустимо пълно отпадане на всяка една от предоставяните услуги.
2.7. Права и задължения на Клиента:

2.7.1. Клиентът има право да получи неизключително и непрехвърляемо право, за срока на договорните отношения, за използването на софтуерните продукти.
2.7.2. Клиентът има право да получава отдалечена поддръжка на Услугата.
2.7.3. Клиентът се задължава да деактивира всяка съществуваща антивирусна програма, система, софтуер и т.н., която е инсталирана на Устройствата преди момента на инсталация на лицензиите, свързани с ползването на Услугата.
2.7.4. Клиентът се задължава да инсталира софтуерните агенти върху Устройствата самостоятелно, за което А1 предоставя файл със софтуерните агенти през споделено пространство за споделяне на файлове.
2.7.5. Ако Клиентът не може да се справи, се обръща за съдействие към екипа на А1 България като използва една от следните контактни точки: support@a1.bg или на телефон 088 1515. В тази случай, служител на А1 България извършва инсталацията на агентите на устройствата на Клиента през софтуер за дистанционно управление AnyDesk. В случай, че това приложение не може да се стартира на устройствата на Клиента, специалисти на А1 извършват посещение на адреса/адресите на Клиента и правят инсталацията директно на устройствата. За извършването на тази дейност се подписва Протокол за извършена дейност във връзка с предоставяне на услугите от Пакет Киберсигурност.
2.7.6. Клиентът се задължава да осигури изпълнение на всички системни изисквания за нормална работа на софтуера, които са налични в интерфейса на платформата.
2.7.7. Клиентът се задължава да осигури на А1 и на неговите служители или посочени от него лица всички условия, необходими за изпълнението на Услугата – всякаква техническа информация и съдействие във връзка с изграждането и конфигурирането на Услугата, достъп до свои помещения и сгради, във време, съвместно уговорено между страните, с оглед изпълнение на задълженията на А1.
2.7.8 Ако е заявена инсталация на софтуерните агенти от А1, Клиентът се задължава да предостави на специалистите на А1 административен достъп до неговите устройства с цел предоставяне на Услугата.
2.8. Стандартни политики за защита:

Посочените Стандартни политики за защита се прилагат на всички клиенти и по отношение на всички софтуерни агенти за Endpoint Protection SentinelOne при първоначалната активация на Услугата. Промени по тези политики се правят само след писмена заявка от клиента по имейл към support@a1.bg и ITManagedServices@a1.bg. Промяната в политиките се извършва в рамките на до три работни дни от датата на получаване на заявката от звеното по поддръжка на Услугата в А1 България.		
ТИП ЗАЩИТА		
Заплаха Threat	Описание	Опция Option
Malicious Threat / Злонамерена атака	Действия, които се предприемат от агента при откриване на зловредна заплаха	Protect / Защитаване
Suspicious Threat / Подозрително действие	Действия, които се предприемат от агента при откриване на подозрителна заплаха	Detect / Откриване на заплаха
Ниво на защита Protection Level	Описание	Опция Option
Kill & Quarantine / Спиране на процеса и карантиниране	При откриване на заплаха се "убиват" процесите и се карантинират се файловете, свързани със заплахата	Enabled / Включено

Remediate / Коригиране	Изтриване на файловете свървани със заплахата и връщане на промените по операционната система от преди атаката	Enabled / Включено
Rollback / Връщане на устройството в състояние от преди атака	При Windows OS се използва VSS, за възстановяване на операционната система в последното стабилно състояние (Windows)	Enabled/ Включено
Containment / Ограничаване	Устройството, на което е открита заплаха се "разкача от мрежата", т.е. агента блокира изцяло мрежовия трафик, с изключение на достъпа на агента до конзолата и обратно	Disabled / Изключено
Агент/ Agent		
Настройки за защита Security Settings	**Описание**	**Опции Option**
Anti Tamper / Забрана за промени	Не дава възможност на потребителя да прави промени локално по агента	Enabled/ Включено
Snapshots / Създаване на backup	Използва се VSS технологията на Windows, за създаване на бекъп на системата. Използва се при опцията Rollback	Enabled/ Включено
Logging / Запазване на логове в системата	Запазват се логове, локално на системата с цел по-добро оказване на съпорт	Enabled/ Включено
Scan New Agents / Сканиране на ОС при ново - инсталирани агенти	Пълно сканиране на операционната система при инсталиране на агента	Enabled/ Включено
Потребителски интерфейс на агента/ Agent UI		
Настройки на потребителския интерфейс на агента Agent UI Settings	**Описание**	**Опции Option**
Show Agent UI & tray icon on endpoints	Показване на агента в лентата за задачи на съответната операционна система	Enabled/ Включено
Show pop-up notifications for Threats and Mitigation	Показване на изскачащи съобщения при блокиране на заплахи (Windows, MacOS)	Enabled/ Включено

Show pop-up notifications for Blocked Devices	Показване на изскачащи съобщения при блокиране на външни устройства (Windows, MacOS)	Enabled/ Включено
Show suspicious events in the UI	Показване на подозрителни заплахи в UI на агента	Enabled/ Включено
Show warning in case of Agent errors	Функционалните предупреждения, се показват като съобщения за операционната система (Windows, MacOS)	Disabled / Изключено
Show in the UI events from the last N days	Заплахи по-стари от посочения брой дни, не се визуализират в UI на агента (Windows, MacOS)	30 days
Show these menu items in the UI	Показване на следните елементи в UI /User Interface/ на Агента	
- Blocked Devices	Показване на блокирани устройства в UI на агента	Disabled / Изключено
- Quarantined Files	Показване на карантинирани файлове в UI на агента	Enabled/ Включено
- Contact Support	Показване на информация за контакт със сънорт	Disabled / Изключено
Support Contact Information	Информация за поддръжка	
- Free Text Message	Текстово съобщение	Disabled/ Изключено
- Company or Org	Компания	Disabled/ Изключено
- Phone Number	Телефонен номер	Disabled/ Изключено
- Direct Message	Директно съобщение	Disabled/ Изключено
- Support Website	Уебсайт	Disabled/ Изключено
- Other	Допълнителен текст	Disabled/ Изключено
Deep Visibility		
Configuration	Описание	Option
Enable Deep Visibility	Включване на възможностите на агента за Deep Visibility	Disabled/ Изключено
Други Опции/ More Options		
Опции Option	Описание	Опции Option
Decommissioning	Премахване на агента от конзолата за управление след посочения брой дни	Enabled - 21 days / Включено след 21 дни
Remote Shell	Възможност за осигуряване на отдалечен powershell достъп до работната станция или сървъра, на който е инсталиран агента	Disabled/ Изключено

2.9. Предоставяне на услугата:

2.9.1. Служител на А1 създава профил на Клиента в Платформата в рамките на 10 (десет) работни дни от датата на сключване на Договора.

2.9.2. А1 предоставя на Клиента идентификационните данни за достъп до Платформата в срок до 2 (два) работни дни от създаване на Клиентския профил, както и номер на услуга към чиято сметка ще се заплаща Услугата, в случай че не е посочен в съответното приложение.
2.9.3. А1 осигурява използването на Услугата в срок до 60 (шестдесет) работни дни от датата на подписване на Договора.
2.9.4. Клиентът инсталира софтуерните агенти на устройствата си и или се обръща към А1 на имейл support@a1.bg или на телефон 088 1515 за съдействие с инсталацията. Инсталацията се извършва чрез дистанционен достъп до устройствата на Клиента, като същият се задължава да предостави административен достъп до устройствата на специалистите на А1.

1. Услугата включва следните дейности: 1.1. Създаване на профил на Клиента в конзолата за управление на услугата; 1.2. Алокиране на заявения брой лицензи от съответния вид в профила на Клиента; 1.3. Генериране и предоставяне на Клиента на софтуерен агент, който да бъде активиран на всяко защитавано устройство; 1.4. Налагане на стандартна политика за защита; 1.5. Промени по конфигурацията и настройките и дейности по добавяне на нови потребители в срока на Договора: до 4 човекочаса месечно на ниво компания при закупени само Complete пакети. 2. Броят човекочасове е фиксиран за вида пакет и не е обвързан с броя на активирани пакети от Клиента. 3. В дейностите, които са включени в посочените човеко-часове не са включени анализи на резултати от EDR докладите и данни от Thread Hunting.
2.12. Нива на поддръжка
1. Поддръжка на ниво 1: 1.1. Събиране на подходяща информация. 1.2. Идентифициране и анализ на проблеми. 1.3. Първоначална диагноза. 1.4. Отстраняване на неизправности. В тази дейност не са покрити активности, които касаят крайните устройства на Клиента, до които А1 няма административен достъп. 1.5. Разрешаване на проблеми, свързани с услугата, където е възможно. В тази дейност не са покрити активности, които касаят крайните устройства на Клиента, до които А1 няма административен достъп. 1.6. Времето за реакция на А1 за поддръжка от ниво 1 не трябва да надвишава 48 часа. 2. Поддръжка на ниво 2 2.1. Отстраняване на неизправности и диагностика. 2.2. Потенциално репликиране на проблема в тестова лабораторна среда. 3. Условията за поддръжка на SentinelOne на https://www.sentinelone.com/legal
2.13. Политики при конфигурация на услугата и политика за защита
1. А1 създава профил на Клиента в конзолата за управление на услугата, като активира стандартна политика: При идентифицирани като malicious атаки, услугата извършва протекция, т.е. блокира атаките. При идентифициране на събития, квалифицирани като подозрителни, услугата генерира информация в конзолата за това събитие, но действието ще бъде пропуснато. 2. А1 не носи отговорност за въведените политики на защита, в случай, че на Клиента е предоставен Admin достъп до платформата за управление на услугата. В този случай, отговорността на А1 отпада, тъй като типът на достъпа предоставя на Клиента

възможност по всяко време и извън контрола на А1 да въвежда промени в политиките за защита.
3. Ползване на лицензите влиза в сила от датата на активиране на лицензите в платформата на SentinelOne Inc., като Срокът на ползване е съгласно Договора.
4. Страните приемат Стандартни политики за защита, посочени в Приложение № 2 към Договора, приложими за всички клиенти и по отношение на всички софтуерни агенти за А1 Endpoint Protection при първоначалната активация на услугата. Промени по Стандартните политики за защита са допустими само след писмена заявка от Клиента на имейл: support@a1.bg и ITManagedServices@a1.bg. Промяната в Стандартните политики за защита се извършва от А1 в срок до 3 (три) работни дни от датата на получаване на съответната заявка за промяна.
5. При идентифициране на спряна („карантинирана“) софтуерна програма в резултат на коректното действие и превенция на политиките за защита, конфигурирани в платформата, Клиентът има право да изключи програмата от карантина/спиране (exclusion) единствено след писмена заявка до А1 на имейл: support@a1.bg и ITManagedServices@a1.bg.

3. Cyber Backup

3.1. Услугата А1 Cyber Backup се предоставя като продукт – част от избрания Пакет Кибесигурност. Услугата предоставя на Клиента възможност да създава резервно копие на своите данни и да ги съхранява в в център за данни на А1. Всички настройки, свързани с използването на Услугата се извършват в единен портал, до който Клиентът получава достъп след подписване на Договора.
3.2. Услугата се предоставя от А1 БЪЛГАРИЯ ЕАД, в качеството му на оторизиран представител на Acronis International GmbH (Acronis) в съответствие с (а) условията на Договора, приложенията, тези Правила, Общи условия за информационно-комуникационни технологични (ICT) услуги, предоставяни от А1 БЪЛГАРИЯ ЕАД и (б) Условията на Acronis.
3.3. Услугата се ползва при следните условия:
3.3.1. Служител на А1 създава профил на Клиента в портал на Acronis.
3.3.2. За целите на ползване на Услугата, Клиентът определя лице за контакт и посочва верен и актуален имейл адрес, на който А1 предоставя идентификационни данни за достъп до портала за управление на Услугата.
3.4.3. А1 предоставя на Клиента идентификационните данни за достъп до портала за управление, както и активен идентификационен номер на услуга от А1 (А1 Номер).
3.4.4. След създаване на Клиентския профил, специалисти на А1 въвеждат стандартни настройки на Услугата чрез портала и
3.4.5. Служител на А1 България или администратор на Клиента инсталира софтуерни агенти на съответните устройства, които трябва да бъдат защитени. Ако Клиентът не може да се справи, се обръща за съдействие към екипа на А1 България като използва една от следните контактни точки: support@a1.bg или на телефон 088 1515. В тази случай, служител на А1 България извършва инсталацията на агентите на устройствата на Клиента през софтуер за дистанционно управление AnyDesk. В случай, че това приложение не може да се стартира на устройствата на Клиента, специалисти на А1 извършват посещение на адреса/адресите на Клиента и правят инсталацията директно на устройствата. За извършването на тази дейност се подписва Протокол за извършена дейност във връзка с предоставяне на услугите от Пакет Киберсигурност.

3.4.6. Клиентът започва да я ползва по реда и начина, предвидени в Условията на Acronis и настоящите Условия.
3.4.7. Клиентът няма право да прави промени в конфигурацията на Услугата самостоятелно, освен след заявка към първо ниво на поддръжка на имейл support@a1.bg или на телефон 088 1515.
3.5. Включени функционалности

Портал за управление на A1 Cyber Backup, чрез който се въвеждат всички настройки за пълноценно използване на включените функционалности, е достъпен на следния интернет адрес: https://cloud.acronis.com/login.	
Бекъп на данни, приложения и системи	• Бекъп на устройства – работни станции (desktop и laptop), сървъри, виртуални машини • Бекъп на файлове • Бекъп на ниво операционна система • Бекъп на всички често използвани бизнес приложения • Бекъп на споделени папки
Пълно описание на функционалностите на софтуера за управление на Услугата е публикувано на интернет страницата на Acronis, на следният интернет адрес: https://www.acronis.com/en-us/support/documentation/CyberProtectionService/#welcome-to-cyber-protection.html	
3.6. Срокове за изпълнение	
Срок за създаване на профил на Клиента	10 (десет) работни дни от датата, на подписване на Договора
Срок за предоставяне на идентификационните данни за достъп до портала за управление, както и активен идентификационен номер на услуга от A1 (A1 Номер), към чиято сметка (фактура) се заплащат Услугите по Договора	2 (два) работни дни от създаване на Клиентския профил,
3.7. Дейности • Приемане на заявки и въпроси от Клиента. • Регистриране на проблем на Клиента в система на A1 • Регистриране на проблем на Клиента с ползване на портала за управление на A1 Cyber Backup • Разрешаване на основни проблеми като рестартиране на системи, достъпи за Клиента, ресет на пароли, проверка на наличие на обслужващите Услугата системи и софтуер, както и други базови действия. • Препращане към следващо ниво на поддръжка, когато проблемът е по-сложен или изисква специализирани познания и достъп до технически системи и платформи, чрез които се предоставя услугата. • Проследяване на инциденти и следене за спазване на времена за реакция и разрешаване на проблеми. • Документиране на заявките: Записване на детайли за заявките и предоставяне на информация на следващите нива на поддръжка	

3.8. Условия и правила за ползване:

3.9. Клиентът получава достъп за администриране на услугата след активирането ѝ в платформата чрез определено от него и посочено в Договора лице ("Администратор"). Въпреки това, администрирането на услугата се извършва от специалисти на А1 България. Ако Клиентът извършва самостоятелно настройки промени по вече въведени настройки в платформата за администриране на Услугата, същият носи изцяло отговорност за действията на Администратора и за активираните от последния функции, промени и добавени пакети, в това число за тяхното заплащане. С оглед избягване на всякакво съмнение: А1 не носи отговорност за каквито и да са недобросъвестни действия, свързани с администриране на услугата, извършено от името и за сметка на Клиента (чрез негови имена/ пароли).

3.10. За да бъде използвана услугата А1 Cyber Backup /Managed Backup/, се изисква Клиентът да разполага с интернет достъп. За коректна работа на услугата е необходимо следните портове да са отворени в защитните стени на Клиента на ниво мрежа и на самите PC, на които ще се инсталира Cyber Backup софтуерен агент: outbound: TCP портове: 443, 8443, рейндж: 7770–7800, 44445, 55556; inbound: TCP портове: 6888, 18018, 18019; UDP портове: 6888, 6771. Ако тази конфигурация не бъде извършена, А1 не поема отговорност за коректна работя на услугата.

3.11. А1 не поема отговорност при невъзможност за достъп до или неизправност на услугата, в резултат на проблеми, свързани с мрежовата свързаност на Клиента, предоставена от друг доставчик, различен от А1.
3.11. А1 не носи отговорност за клиентското съдържание, ползвано от Клиента чрез услугата А1 Cyber Backup /Managed Backup/ и неговото съответствие с действащите нормативни изисквания.
3.12. А1 не носи отговорност за данни, които се съхраняват на устройства, на които не е инсталиран софтуерен агент за услугата, независимо от причината за това.
3.13. За услугата в платформата на Acronis се конфигурира стандартен план за бекъп /protection plan/ на информацията със следните параметри:

3.13.1. Бекъп на цялата машина в облака в дейта център на А1, който се извършва еднократно в рамките на денонощието от понеделник до петък в 15.00 часа в съответния ден и добавя инкрементъл информацията.

3.13.2. Бекъпира се всичко от директория c:\Users – всички потребителски профили в тази директория

3.13.3. Избира се опция бекъп на файлове и папки

3.13.4. Пазят се две копия на бекъпа назад

3.13.5. Всички функционалности за сигурност са изключени, тъй като се поемат от софтуерните агенти на Endpoint Protect SentinelOne услугата.

3.13.6. Функцията за криптиране е изключена.

3.14. При необходимост от въвеждане на друг вид конфигурация, същата се заявява от Клиента по някой от горепосочените методи за контакт с екипа на А1. Конфигурацията се извършва в срок от 5 работни дни от заявката.

3.15. При прекратяване на Договора по вина на Клиента неговите данни, свързани с ползването на услугата (Клиентските данни) се съхраняват за срок от 30 (тридесет) дни от датата на спиране на достъпа до услугата. След изтичане на посочения срок, тези данни се заличават.
3.16. При прекратяване на Договора по отношение на Услугата с предизвестие, Доставчикът съхранява Клиентските данни до изтичане на срока на предизвестието. След изтичането на срока на предизвестието Клиентските данни, свързани с ползването на Услугата, се заличават безвъзвратно.

4. ОБУЧЕНИЕ ПО КИБЕРСИГУРНОСТ / SECURITY TRAINING

4.1. Услугата SECURITY TRAINING осигуряване на достъп до платформа за провеждане на обучения по отношение на киберсигурността и безопасно използване на интернет („Платформа/та“) чрез линкове, базирани на Universally Unique Identifier (UUID). Чрез достъпните в Платформата обучения (за краткост „Обучение/я“) се осигурява повишаване на дигиталната грамотност по отношение на киберсигурност и безопасно използване на интернет чрез обучение в различни аспекти като разпознаване на социални инженерни атаки, сигурност на паролите, опазване на личната информация, разпознаване на заплахи и рискове и др. Услугата се предоставя в съответствие с условията на Договора и приложенията към него, тези Условия, с Общите условия за информационно-комуникационни технологични (ICT) услуги, предоставяни от А1 БЪЛГАРИЯ ЕАД (Общите условия) и Общите условия за ползване на услугите за достъп до онлайн платформа https://exercybe.com/terms-conditions-bg .
4.2. Клиентът не придобива права на собственост върху Платформата и/или съдържанието, които се предоставят и използват от Клиента.
4.3. Услугата се предоставя за до броя посочени от Клиента лица, които ще преминат Обучение. Броят лица е равен на броя потребители съгласно избрания Пакет, посочен Договора.
4.4. В изпълнение на задълженията си, Доставчикът осигурява:
4.4.1. достъп до следните модули на Платформата:

- Модул 1: 1 бр. основно обучение с вкл. сертификат за преминато обучение
- Модул 2: 24 бр. микрообучения + 1 бр. опреснително обучение от Модул 1 (при поискване)
- Модул 3: 12 бр. бюлетина по киберсигурност
- Модул 4: тест за разпознаване на фишинг атаки и социално инженерство
- Модул 5: симулации за разпознаване на фишинг атаки и социално инженерство, с обучителни портали и тест към тях

4.5. Условия за предоставяне
4.5.1. Достъп до Платформата се осигурява и осъществява, както следва:
4.5.1.1. Достъпът до Модул 1 от Платформата се осъществява по следния начин:
• Доставчикът генерира достъпни от интернет индивидуални линкове в Платформата за конкретните потребители, базирано на email адреси и/или имена на потребителите;
• Клиентът определя отговорно от негова страна лице, наречено Координатор, което получава линковете на предварително дефиниран email адрес, посочен в настоящия Договор;
• Координаторът разпраща индивидуалните линкове на email адресите на съответните потребители;
• Потребителите достъпват линковете и преминават обучението и теста;

4.5.1.2. Достъпът до опреснителното обучение и до останалите модули на Платформата се осъществява по същия начин.4.5.1.2. Срокът за предоставяне правото на ползване на Платформата е 36 (на осигуряване на достъп от страна на Доставчика.
4.5.1.3. За целите на осигуряване на достъп Клиентът предоставя информация за имената на лицата, които ще преминат обучение, в срок до 10 дни след сключване на Договор.
4.5.1.4. Доставчикът осигурява достъп до Модул 1 в срок до 30 дни от датата на подписване на Договор, при условие, че Клиентът е осигурил информацията по чл. 2.4. в определения срок. Предоставянето на достъп се удостоверява с Протокол за приемане на услугата.
4.5.1.5. За целите на ползване на Услугата Клиентът определя лице за контакт - Координатор и лице, което ще получи Доклад за резултатите от преминатото обучение и тест и посочва имейл адрес.
4.5.1.6. При предоставяне и ползване на Платформата Страните се задължават да спазват условията по т.1. и следващите.
4.5.1.7. Клиентът декларира, че е запознат и е съгласен с условията на Общите условия за ползване на услугите за достъп до онлайн платформа https://exercybe.com/terms-conditions-bg .
4.5.1.8 След осигуряването на достъп по реда на чл. 2., всяко лице самостоятелно активира достъп до Платформата и я ползва по реда и начина, предвидени в Общите условия на „РАДЕСОЛ България" ООД.
Клиентът се задължава да използва Платформата по предназначение, съгласно Общите условия, Общите условия на „РАДЕСОЛ България" ООД и инструкциите на Доставчика.
4.6. Клиентът се задължава да не препраща получените индивидуални линкове на други email адреси по никаква причина и да не ги предоставя на трети лица, както и да изиска от служителите си да не осъществяват действията по този чл.

5. ПРЕДОСТАВЯНЕ НА ДОКУМЕНТИ ЗА ПОЛИТИКА ЗА КИБЕРСИГУРНОСТ

5.1. Услугата се предоставя като продукт – част от избрания Пакет Киберсигурност.
Услугата се състои в създаване и предоставяне от страна на Доставчика на набор от документи, които могат да варират в зависимост от типа и мащаба на клиента. Например документи от следния тип:
1) Политика за информационна сигурност
2) Политика За физически достъп до обекти, сървърни помещения и др.
3) Управление на достъп до ресурси - от локалната мрежа и отдалечено
4) Управление на промени в информационните системи
5) Управление на мрежова сигурност
6) Контрол на крайните устройства и защита от зловреден софтуер
7) Потика за резервиране и възстановяване на данните
8) Политика за управление на доставчици
9) Правила за инсталация и използване на софтуер
Списъкът може да варира при промяна в условията на предоставяне.

5.2. Списъкът с документи варира в зависимост от мащаба на съответния бизнес на Клиента и броя на неговите служители.

5.3. Документите се предоставят на хартиен носител или се споделят чрез приложение за споделяне на файлове с оторизирано лице от страна на Клиента от записаните в Договора.

Настоящите ПРАВИЛА И УСЛОВИЯ ЗА ПОЛЗВАНЕ НА ПАКЕТ КИБЕРСИГУРНОСТ Влизат В сила на 12 НоемВри 2024 год.
Настоящите Общи условия са изготВени на български език.