|  |  |
| --- | --- |
| **ПРАШАЛНИК ЗА САМООЦЕНУВАЊЕ ЗА ШЕМА ЗА СЕРТИФИКАЦИЈА**  **„САЈБЕР ОДГОВОРНА ОРГАНИЗАЦИЈА“**  **ОБРАЗЕЦ ВЕРЗИЈА 1.1 ОД 09.12.2021 ГОДИНА** |  |

 Сите полиња во овој образец се задолжителни за пополнување, освен ако не е поинаку наведено во називот на полето.

**Општи информации**

Во овој дел, треба да ги внесете општите информации за вашата организација.

A.1.1 Назив на организација

Click or tap here to enter text.

А.1.2 Телефонски број

Click or tap here to enter text.

A.1.3 Регистарски (матичен) број

Click or tap here to enter text.

A.1.4 Адреса на организација

Click or tap here to enter text.

Внесете ја адресата за седиштето на вашата организација, како што е запишано во Централен регистар

А.1.5 Дејност на вашата организација

Click or tap here to enter text.

Внесете шифра и назив за главната дејност на организацијата, како и забелешка ако е потребно.

A.1.6 Адреса за веб-седиште на организацијата

Click or tap here to enter text.

Внесете URL адреса за вашата главна веб-страница.

А.1.7 Име и Презиме на одговорно лице во организацијата

Click or tap here to enter text.

Ова е лицето кое пред поднесување на пополнетиот прашалник ќе треба електронски да го потпише генерираниот PDF документ.

А.1.8 Емеил адреса

Click or tap here to enter text.

Емеил адреса на одговорно лице во организацијата кое ќе биде задолжено за потпишување на прашалникот со дигитален сертификат.

А.1.9 Големина на организацијата

Mикро (<10 вработени)

Мали (<50 вработени)

Средни (<250 вработени)

Големи

А.1.10 Колку вработени работат од дома

Click or tap here to enter text.

Внесете број на вработени или ангажирани лица кои континуирано работат од дома.

А.1.11 Дали за прв пат поднесувате барање за сертификација или обновувате претходно издаден сертификат?

Прв пат

Обнова

Изберете од листата.

А.1.12 Која е главна причина за поднесување на барањето?

Потребно за комерцијален договор

Потребно за државен договор

Потребно од клиент

Потребно од осигурител

Потребно од регулаторно тело

Потребно за грант

За исполнување барања за заштита на податоци за исполнување барања за заштита на податоци

Генерално да ја подобруваме нашата безбедност

Друго

Click or tap here to enter text.

Ве молиме, кажете ни ја главната причина зошто аплицирате за сертификација. Ако има повеќе причини, изберете ја онаа што ви е најважна. Ова ни помага да разбереме како луѓето ги користат нашите сертификати.

**Опсег на барањето**

Во овој дел, треба да ги опишете функционалните делови од вашата организација што сакате да ги опфатите со барањето. Опсегот треба да биде или целата организација или организациска единица, или повеќе делови на една или повеќе различни географски локации. Сите компјутери, лаптопи, сервери, мобилни телефони, таблети и заштитни ѕидови / рутери што можат да пристапат на Интернет и се користат од оваа организација или единица за пристап до деловни информации, треба да се сметаат за „опсег“. Сите локации што се во сопственост или управувани од организацијата или единицата, без разлика дали се во Република Северна Македонија или на меѓународно ниво, треба да се сметаат дека се „во опсег“.

А.2.1 Дали опсегот на оваа проценка ја опфаќа целата ваша организација?

Choose an item.

Целата ваша организација ќе ги вклучува сите организациски единици, подружници, и сите луѓе и уреди што користат деловни податоци.

A.2.2 Ако опсегот не е целата организација, тогаш каков опис на опсегот би сакале да се појави на вашиот сертификат и на веб-страницата?

Click or tap here to enter text.

Вашиот опис за опсег треба да дава детали за сите области на вашиот бизнис што имаат пристап до Интернет и тие што евентуално се исклучени од шемата за сертификација (на пример, „цела компанија без развојна мрежа“)

A.2.3 Ве молиме, опишете ги географските локации на вашата организација што се во рамките на ова барање.

Click or tap here to enter text.

Треба да наведете општ опис, сите канцеларии во земјата или едноставно да ги наведете по број локациите. Пример: Малопродажба во Скопје и Битола.

A.2.4 Ве молиме наведете ги количините на лаптопи, компјутери и сервери во рамките на оваа проценка. Мора да вклучите верзии на модели или години старост и оперативни системи за сите уреди.

Click or tap here to enter text.

Ве молиме, наведете резиме на сите лаптопи, компјутери и сервери што се користат за пристап до деловни податоци и имаат пристап до Интернет (на пример, „Имаме 25 лаптопи кои работат на Windows 10 верзија 1709). Не треба да давате сериски броеви, MAC адреси или дополнителни технички информации.

A.2.5 Ве молиме наведете ги количините на таблети и мобилни уреди во рамките на оваа проценка. Мора да вклучите верзии на модели, години старост и оперативни системи за сите уреди.

Click or tap here to enter text.

Сите таблети и мобилни уреди што се користат за пристап до деловни податоци и имаат пристап до Интернет, мора да бидат вклучени во опсегот на проценката. Не треба да давате сериски броеви, мак адреси или други технички информации.

A.2.6 Ве молиме, наведете список на мрежи што ќе бидат во опсегот на оваа проценка.

Click or tap here to enter text.

Треба да вклучите детали за секоја мрежа што се користи во вашата организација, вклучувајќи го нејзиното име, локација и нејзината намена (т.е. Главна мрежа во Централата за административна употреба, јавна Wi-FI мрежа за посетители и сл.) Не треба да давате IP адреси или други технички информации.

A.2.7 Ве молиме, наведете список на мрежна опрема што ќе биде во опсегот на оваа проценка (вклучително и заштитни ѕидови и рутери).

Click or tap here to enter text.

Треба да ја вклучите целата опрема што го контролира протокот на податоци, како што се рутери и заштитени ѕидови. Не треба да вклучувате свичеви или безжични пристапни точки за пристап што не содржат заштитен ѕид или не го насочуваат сообраќајот на Интернет.

A.2.8 Ве молиме наведете го името и улогата на лицето кое е одговорно за управување со информациските системи на организацијата во рамките на оваа проценка?

Click or tap here to enter text.

Ова треба да биде лицето кое влијае и донесува одлуки за компјутерите, лаптопите, серверите, таблетите, мобилните телефони и мрежната опрема во вашата организација. Ова лице мора да биде вработено во вашата организација и не може да биде лице од вашиот добавувач на ИТ-услуги.

**Безбедно деловно работење**

**Огнени (заштитни) ѕидови / Firewalls.**

Канцелариски огнени (заштитни) ѕидови (Firewalls) и излезни точки кон Интернет (internet Gateways). Заштитен ѕид (огнен ѕид - firewall) е општо име за софтвер или хардвер што обезбедува техничка заштита помеѓу вашите системи и надворешниот свет. Во вашиот интернет рутер ќе има заштитен ѕид. Вообичаено рутерот и заштитниот ѕид се опрема што може да ви ја достави на користење Интернет провајдерот како дел од користење на Интернет услугата. Вашата организација, исто така, може да постави посебен хардверски заштитен уред помеѓу вашата мрежа и Интернет. Заштитените ѕидови се моќни уреди и треба правилно да се конфигурираат за да обезбедат ефективна безбедност.

Прашањата во овој дел се однесуваат на: уредите за хардверски заштитен ѕид, рутери, компјутери и лаптопи.

А3.1 Дали имате заштитен ѕид на границите помеѓу внатрешните мрежи на вашата организација и интернетот?

Choose an item.

Мора да имате заштитни ѕидови помеѓу вашата канцелариска мрежа и Интернет. Исто така, треба да имате заштитени ѕидови за надворешен пристап на ваши вработени до организацијата, како на пр. домашни работници. Вообичаено е надворешните корисници да пристапуваат до организациска мрежа преку активна услуга за Виртуелна приватна мрежа (VPN), достапна како дел од заштитниот ѕид.

А.3.2 Кога за прв пат добивате интернет рутер или хардверски заштитен ѕид, уредот ќе има стандардна лозинка. Дали оваа првична лозинка е променета на сите такви уреди? Како го правите ова?

Click or tap here to enter text.

Стандардната лозинка мора да се смени на сите рутери и заштитени ѕидови, вклучително и на оние што доаѓаат со почетна претходно конфигурирана лозинка (на пр. Wi-Fi рутер од интернет-провајдер) Може да ја промените стандардната лозинка со најавување на веб-интерфејсот за уредот (често лоциран на 192.168.1.1) или 127.0.0.1)

А.3.3 Дали новата лозинка на сите ваши интернет рутери или хардверски заштитен ѕид е долга најмалку 8 карактери и тешко е да се погоди?

Choose an item.

Лозинката што е тешко да се погоди треба да биде единствена, да не биде составена од вообичаени или предвидливи зборови, како што се „лозинка“ или „администратор“, и да не вклучува предвидливи секвенци како „12345“.

А.3.4 Дали ја менувате лозинката кога верувате дека можеби е компромитирана? Како го постигнувате ова?

Click or tap here to enter text.

Лозинките може да бидат компромитирани ако имало вирус на вашите уреди и системи или ако производителот на опремата Ве извести за безбедносна слабост на нивниот производ. Треба да бидете свесни за ова и да знаете како да ја смените лозинката доколку се случи тоа.

А.3.5 Дали имате овозможени услуги што се достапни однадвор преку вашите интернет рутери или хардверски заштитен ѕид, за кои немате документиран деловен случај, т.е. пишан опис за намената и целите на услугите со бараните подесувања?

Choose an item.

А.3.6 Ако имате овозможени услуги на вашиот заштитен ѕид, дали имате процес да се осигурате дека тие се навремено оневозможени кога веќе не се потребни? Опишете го процесот. Се пополнува само ако на А.3.5 е одговорено со ДА)

Click or tap here to enter text.

Ако веќе не ви е потребно одредена услуга да е овозможена и достапна преку вашиот заштитен ѕид, мора да ја отстраните за да го намалите ризикот од компромитација и хакерски упад. Треба да имате процес што го следите за да го направите ова (т.е. кога се разгледуваат услугите, кој одлучува да ги отстрани услугите, кој проверува дали тоа е сторено)

А.3.7 Дали сте ги конфигурирале вашите интернет рутери или хардверски заштитен ѕид, така што тие ги блокираат сите други услуги што не се користат да не се достапни на Интернет?

Choose an item.

Стандардно, повеќето заштитени ѕидови го блокираат пристапот на сите услуги од Интернет, но треба да ги проверите поставките за заштитен ѕид.

А.3.8 Дали вашите Интернет рутери или хардверски заштитни ѕидови се конфигурирани да овозможуваат пристап до нивните поставки за конфигурација и администрација на самиот уред преку Интернет?

Choose an item.

Понекогаш организациите го конфигурираат својот заштитен ѕид за да им дозволат на другите (како на пр. што е компанија за ИТ поддршка) да ги менуваат поставките преку Интернет. Ако не сте ги поставиле заштитните ѕидови да бидат достапни за луѓе надвор од вашите организации или поставките за конфигурација на уредот се достапни само преку VPN конекција, тогаш одговорете „не“на ова прашање.

А.3.9 Ако да, дали има документирано деловно барање за овој пристап? (Се пополнува само ако на A.3.8 е одговорено со Да)

Choose an item.

Сигурно сте донеле одлука во организацијата дека треба да обезбедите надворешен пристап до вашите рутери и заштитни ѕидови. Оваа одлука мора да биде документирана (т.е. запишана).

А.3.10 Ако да, дали пристапот до поставките е заштитен со автентикација со два фактори или со дозволување само на доверливи IP адреси пристап до поставките? Наведете која опција се користи. (Се пополнува само ако на А.3.8 е одговорено со Да)

Click or tap here to enter text.

Ако дозволите директен пристап до поставките за конфигурација преку вашиот рутер или надворешен интерфејс на заштитен ѕид, ова мора да биде заштитено со една од двете опции.

А.3.11 Дали имате овозможено софтвер за заштитен sид на сите ваши компјутери и лаптопи?

Choose an item.

Оваа поставка можете да ја проверите на Mac во делот Безбедност и приватност во Системските преференци. На лаптопите за Виндоус можете да го проверите ова со одење во „Поставки“ и пребарување за „Windows Firewall“. На Linux пробајте со команда „status ufw“. Може да користите и заштитен ѕид што може да го обезбеди вашиот антивирусен софтвер.

**Безбедни конфигурации**

Со основна стандардна инсталација и на поетокот на користењето, компјутерите, рутерите и другите информатички и мрежни основни средства најчесто не се доволно заштитени. Тие често можат да вклучуваат административна сметка со коринисчко име Admin и стандардна, јавно позната лозинка, како и овозможена една или повеќе дополнителни и непотребни кориснички сметки (често со високи нивоа на пристап и привилегии) и претходно инсталирани, но непотребни програми, апликации или услуги (т.н. bloatware).Сите тие претставуваат безбедносни ризици кои организацијата треба да ги сведе на минимум.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети и мобилни телефони.

А.4.1 Дали на вашите лаптопи, компјутери, сервери, таблети и мобилни телефони го отстранивте целиот софтвер што не го користите (секаде каде што е можно)? Опишете како го постигнувате ова.

Click or tap here to enter text.

За да ги видите инсталираните апликации на Windows, погледнете во Start Menu, на macOS отворен Finder-> Applications и на Linux отворете го вашиот менаџер за софтверски пакети (apt, rpm, yum). Мора да ги отстраните или оневозможите сите апликации, системски услуги и мрежни услуги што не се потребни за секојдневно работење.

А.4.2 Дали проверувате дека сите сите компјутери имаат само кориснички сметки што ги користите во тековното работење?

Choose an item.

Мора да отстраните или оневозможите кориснички сметки што не се потребни за секојдневна употреба на сите уреди. Можете да ги прегледувате вашите кориснички сметки на Windows со десен клик на Start -> Computer Management -> Users, на macOS во System Preferences -> Users & Groups, и на Linux користејќи „cat / etc / passwd“

А.4.3 Дали сте ја смениле стандардната лозинка за сите кориснички и административни сметки на сите ваши лаптопи, компјутери, сервери, таблети и паметни телефони во лозинка од 8 или повеќе карактери што тешко може да се погоди?

Choose an item.

Силна лозинка е таа што е тешко да се погоди. Таа треба да е единствена и да не се користи кај повеќе кориснички сметки, и да не е составена од предвидливи зборови, како што се „Password“ или „administrator“, или да вклучува бројни секвенци како „12345678“.

А.4.4 Дали сите вработени и администратори користат лозинки од најмалку 8 карактери?

Choose an item.

Колку е подолга лозинката, толку е потешко за компјутерските криминалци да ја погодат (напади со многубројни пробувања на предвидливи лозинки, т.н. Brute-force напад).

А.4.5 Дали имате апликации или софтвер преку кои се овозможува пристап до чувствителни или важни информации и документи за корисници што пристапуваат преку интернет (како сервер за електронска пошта, пристап преку VPN до документи на организацијата)?

Choose an item.

Вашата организација може да има софтвер што им овозможува на луѓето надвор од компанијата преку Интернет да пристапуваат до информации за вашата организација преку надворешна услуга. Ова може да биде сервер за VPN, сервер за е-пошта или интернет апликација што им ја давате на вашите клиенти како производ или услуга. Во сите случаи, овие апликации обезбедуваат информации доверливи за вашето работење и кои не би сакале да бидат јавно достапни. Ова прашање не се однесува на услугите во облак како што се Google Drive, Office365 или Dropbox. Ако користите само такви услуги и немате ваша сопствена услуга, треба да одговорите НЕ на ова прашање.

А.4.6 Ако да, дали сите корисници на овие услуги користат лозинки од најмалку 8 карактери и дали вашите системи не ја ограничуваат должината на лозинката на помалку од 8 карактери? (Се пополнува ако на А.4.5 е одговорено со Да)

Choose an item.

Колку е подолга лозинката, толку е потешко за компјутерските криминалци да ја погодат (напади со многубројни пробувања на предвидливи лозинки, т.н. Brute-force напад).

А.4.7 Ако да, дали имате обезбедено начин или процедура за промена на лозинки од страна на надворешните корисници но и од организациските администратори, во случај на нивна компромитација? (Се пополнува ако на А.4.5 е одговорено со Да)

Choose an item.

Лозинките може да бидат компромитирани ако имало вирус на вашите системи или ако производител на уредите што ги користите ве извести за безбедносна слабост на нивниот производ. Треба да бидете свесни за ова и да знаете како да ја смените лозинката доколку е потребно.

А.4.8 Ако да, дали вашите системи се поставени на автоматско заклучување на корисничката сметка по пет или помалку неуспешни обиди за најавување или го ограничуваат бројот на обиди за најавување на не повеќе од десет во рок од пет минути? (Се пополнува ако на А.4.5 е одговорено со Да)

Choose an item.

Надворешната услуга што ја давате преку вашите системи на Интернет мора да биде обезбедена со систем за најава со цел да идентификува повеќекратни обиди за најава при внес на погрешно корисничко име или лозинка. На тој начин се намалува можноста за компјутерски криминалци да продолжат да пробуваат различни лозинки (т.н. Brute-force напади) со цел да ги пробијат лозинките и да добијат неавторизиран пристап.

А.4.9 Ако да, дали имате пишана политика за лозинка што се однесува на сите ваши корисници (внатрешни и надворешни), која периодично ја проверувате и ревидирате? (Се пополнува ако на А.4.5 е одговорено со Да)

Choose an item.

Политиката за лозинка мора да содржи: упатства за избор на лозинки што не може да се погодат, да не се користи истата лозинка за повеќе сметки, кои лозинки може да бидат запишани и каде може да се зачуваат, колку често треба да се менуваат, задолжително пријавување на сомнеж за пробиена лозинка, обврска за вработените да не ги споделуваат лозинките со други лица и дали можат вработените да користат апликации за менаџирање со лозинки.

А.4.10 Дали на сите компјутери и ИТ уреди е исклучено „автоматско извршување (auto-run)“ и „автоматско репродукција (auto-play)“ за надворешните USB уреди и оптички дискови. Дали е исклучено автоматско препознавање на мобилен телефон како надворешен USB стик кога е приклучен на компјутерот заради полнење на батеријата?

Choose an item.

Ова е поставка што автоматски го стартува и извршува софтверот на ДВД или мемориски стик. Може да оневозможите „автоматско извршување“ или „автоматско репродукција“ на Windows преку „Поставки/Settings“, на „macOS“ преку „Системски преференции/System preferences“ и на „Linux“ преку апликацијата за поставки за вашата дистрибуција. Прифатливо е да се избере опцијата каде што ќе се побара од корисникот да направи избор за тоа какво дејствие ќе се случи секој пат кога ќе вметне мемориски стик. Ако сте ја одбрале оваа опција, можете да одговорите ДА на ова прашање.

**Надградби и закрпи**

За да ја заштитите организацијата, треба да обезбедите навремено ажурирање на апликативниот и системскиот софтвер, како и на т.н. firmware за сите ИТ уреди и основни средства во организацијата. Ажурирањето подразбира инсталирање нанови закрпи и безбедносни и функционални надоградби. Ако на кој било од вашите уреди кои се во опсег на сертификацијата користите оперативен систем што повеќе не е поддржан од производителот (на пр. Microsoft Windows XP / Vista / 2003, Ubuntu 17.10 или постар) и немате обезбедено редовни надградби од други доверливи извори, тогаш не ги исполнувате условите за успешно оценување. Мобилните телефони и таблетите што се во опсег исто така мора да користат оперативен систем што сè уште е поддржан од производителот. и вклучено ажурирање.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети, мобилни телефони, рутери и заштитени ѕидови

А.5.1 Дали сите оперативни системи на вашите уреди се поддржани од производител или добавувач што доставува редовни поправки и надградби за какви било безбедносни проблеми?

Click or tap here to enter text.

Ве молиме наведете ги оперативните системи што ги користите за да може да се процени и провери дали сите ваши оперативни системи сè уште имаат поддршка од производителите. Постарите оперативни системи што не се поддржани и е потребно да ги надградите или замените вклучуваат Windows XP / Vista / 2003 и Ubuntu Linux 17.10.

A.5.2 Дали сите канцелариски апликации што ги користите во организацијата и кои се инсталирани на вашите уреди се поддржани од снабдувач што редовно објавува поправки и надградби за какви било безбедносни проблеми?

Click or tap here to enter text.

Наведете ги апликациите што ги користите за да се разбере начинот на поставување во вашата организација и за потврда дека сите ваши апликации имаат обезбедена поддршка. Ова вклучува софтверски аплиакции и приклучоци како што се Java, Flash, Adobe Reader и .NET. Дополнително тука спаѓаат и софтверите што се изработени локално за вас.

A.5.3 Дали целокупниот софтвер е лиценциран во согласност со препораките на производителот?

Choose an item.

Целиот софтвер мора да биде лиценциран. Прифатливо е да користите бесплатен и софтвер од тип „отворен извор“ (Open source), сè додека ги исполнувате сите услови за лиценцирање, подмирени права за негово користење и поддршка.

А.5.4 Дали сите важни или критични безбедносни ажурирања за оперативните системи се инсталирани во рок од 14 дена од објавувањето? Опишете како го постигнувате ова.

Click or tap here to enter text.

Опишете. Секоја сајбер одговорна организација задолжително треба да ги инсталира сите вакви надградби во одреден претходно договорен рок, на пр. две недели од денот на објава и јавна достапност од страна на производителот.Ако не можете постојано да го постигнете ова барање, нема да постигнете усогласеност со ова барање. Ова барање се однесува само на високо ризични или критични безбедносни ажурирања и закрпи.

A.5.5 Дали сите важни или критични безбедносни ажурирања за апликациите (вклучително и додатоци како на пример Java или Flash) се инсталирани во рок од 14 дена од објавувањето?

Click or tap here to enter text.

Опишете како го постигнувате ова. Опишете. Секоја сајбер одговорна организација задолжително треба да ги инсталира сите вакви надградби во одреден претходно договорен рок, на пр. две недели од денот на објава и јавна достапност од страна на производителот. Ако не можете постојано да го постигнете ова барање, нема да постигнете усогласеност со ова барање. Ова барање се однесува само на високо ризични или критични безбедносни ажурирања и закрпи.

А.5.6 Дали ги отстранивте од компјутерите и другите ИТ средства оние апликации кои повеќе немаат поддршка од производителот и за кои не можете да добивате редовни надградби и безбедносни поправки?

Choose an item.

Задолжително треба да ги отстраните постарите апликации од уредите во моментот кога ќе дознаете дека производителот веќе не ги поддржува. Таквите апликации може да вклучуваат постари верзии на веб-прелистувачи како Internet Explorer, софтверски додатоци како што се Java и Flash и слично.

**Контрола на пристап**

**Кориснички сметки**

Една сајбер одговорна органзиација треба да го применува правилот за пристап со најниски можни привилегии за корисникот или вработениот да може непречено да ги заврши работните задачи и обврски. Важно е да им се овозможи на корисниците и вработените пристап до сите ресурси и податоци потребни за нивните улоги и работни места, но не и повеќе од потребниот минимум. Сите корисници треба да имаат единствени сметки и не треба да извршуваат секојдневни задачи како што се фактурирање или работа со е-пошта додека се најавени како корисник со администраторски привилегии. Користењето на кориснички сметки со високо ниво на привилегии за извршување на секојдневните задачи е ризик за компромитација на компјутерот и преку него на целата организација. Користењето на „обичните“ кориснички сметки кои немаат привилегии за инсталација на софтвер помагаат да се спречи инфекција на уредот со вирус или друг штетен софтвер.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети и мобилни телефони.

А.6.1 Дали на корисниците им се доделуваат кориснички сметки за пристап и користење на ИТ уредите и апликациите само по претходно одобрување од одговорно лице? Дали имате воспоставено процес за оваа активност? Опишете го процесот.

Click or tap here to enter text.

Мора да се осигурате дека корисничките сметки што се користат за најавувања на компјутерите, како и кориснички или администраторски сметки на сервери, се доделени само откако ќе бидат одобрени од лице со одговорна улога во организацијата.

А.6.2 Дали можете да пристапите до лаптопите, компјутерите и серверите во вашата организација, како и до апликациите што се инсталирани на нив, САМО преку внесување на уникатно корисничко име и лозинка?

Choose an item.

Мора да бидете сигурни дека не може да се пристапи до ниту еден важен уред без да се внесе корисничко име и лозинка. Корисниците не смеат да споделуваат сметки.

А.6.3 Како обезбедувате бришење или блокирање на кориснички сметки, како и раздолжување со компјутер или друг ИТ уред, за вработени кои повеќе не се во вашата организација или смениле работно место?

Click or tap here to enter text.

Кога вработен ќе ја напушти вашата организација, треба да спречите пристап до кој било од вашите системи. Истовремено треба да обезбедите информациите, документите и податоците што ги користел тој вработен да останат во владеење на организацијата како нејзина сопственост, и да обезбедите соодветно евидентирање и предавање на друг вработен кој ја презема неговата позиција. Истото важи и за компјутерите и другите ИТ уреди кои организацијата му ги дала на тој вработен за привремено користење.

А.6.4 Дали обезбедувате дека вработените имаат само привилегии што им се потребни за да ја извршат својата тековна работа? Како го правите ова?

Click or tap here to enter text.

Кога некој вработен го менува работното место, можеби ќе треба да ги промените неговите привилегии за пристап до системите, апликациите, документите и податоците.

**Администраторски сметки**

A.6.5 Дали имате процес за доделување на администраторски пристап до системите и услугите на организацијата за вработено или надворешно ангажирнао лице? Опишете го процесот.

Click or tap here to enter text.

Мора да имате формален, запишан процес што го следите кога одлучувате да му дадете некому пристап до системите на администраторско ниво. Овој процес може да вклучува одобрување од лице кое е сопственик / директор / доверител / одговорно или назначено лице на организацијата.

А.6.6 Како обезбедувате дека вработените користат администраторски сметки само за извршување на администраторски активности (како што се инсталирање на софтвер или правење промени во конфигурацијата)?

Click or tap here to enter text.

Мора да се осигурате дека администраторските сметки се користат само кога е апсолутно неизбежно, како на пример при инсталирање на софтвер. Користењето сметки со администраторско ниво на пристап за извршување на секојдневните активности го изложува уредот на кој е најавен корисникот од компромитација со вирус или друг малициозен софтвер.

А.6.7 Како забранувате користење на администраторските сметки за пристап до е-пошта или прелистување на веб?

Click or tap here to enter text.

Мора да обезбедите администраторските сметки да не се користат за пристап до веб-страници или работа со е-пошта. Користењето на вакви сметки за овие секојдневни и вообичаени активности го изложува уредот на кој е најавен корисникот на компромитација со малициозен софтвер. Организацијата треба да воведе и користи политика и процедура. Корисни се и периодични обуки на вработените.

А.6.8 Дали водите евиденција за тоа кои корисници имаат администраторски сметки во вашата организација?

Choose an item.

Една сајбер одговорна организација треба да води список или да има ажурирана и точна евиденција на сите луѓе на кои им биле доделени администраторски сметки, со податоци за корисничко име, систем, услуга, уред до кој им е доделен администраторскиот пристап, како и електронска евиденција (логови) за користењето на овие кориснички сметки со детали за активноста.

А.6.9 Дали редовно или периодично проверувате и ревидирате кој треба да има администраторски пристап?

Choose an item.

Мора редовно да го прегледувате списокот со луѓе со администраторски пристап. Во зависност од вашето работење, ова може да се прави на одреден временски период, на пр. месечно или годишно. Администраторскиот пристап треба да се оневозможи за сите корисници на кои повеќе не им се потребни администраторски привилегии за да ги извршуваат своите работни задачи.

A.6.10 Дали за администраторски пристап користите дво-факторска автентикација?

Choose an item.

Ако вашите системи поддржуваат автентикација со користење на два фактори (каде покрај лозинката за успешна најава е потребно да добиете текстуална порака, еднократен код, или да користите читач за отпечаток од прст или имате имплементирано препознавање на лице), тогаш треба да го овозможите овој начин за најава и пристап за администраторските сметки.

**Вируси, малициозен софтвер, сајбер напади и инциденти**

**Заштита од малвер**

Малициозен софтвер (како што се компјутерски вируси) обично се користи за кражба на информации или за нанесување на финансиска и друг вид штета на организацијата. Антивирусните и антималвер софтверски решенија се достапни од комерцијални добавувачи, но има и некои што се бесплатни или се дел од пакет, на пр. оперативен систем.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети и мобилни телефони.

А.7.1 Дали сите ваши сервери, компјутери, лаптопи, таблети и мобилни телефони се заштитени од малициозен софтвер со: А - инсталиран анти-малвер софтвер, Б - ограничување на инсталација за само претходно одобрени апликации, или В - со изолација на апликации (т.н. Sandboxing, т.е. со употреба на виртуелна машина)?

A - анти-малвер софтвер

Б - ограничување на инсталација за само претходно одобрени апликации

В - со изолација на апликации (т.н. Sandboxing, т.е. со употреба на виртуелна машина)

Ве молиме, изберете ги сите опции што се користат во вашата организација на сите ваши уреди. Повеќето организации кои користат паметни телефони и стандардни лаптопи ќе треба да ги користат и изберат опциите А и Б.

A.7.2 (А) Таму каде што имате инсталирано антивирус или друг софтвер за заштита од малвер (МАЛициозен софтВЕР), дали истиот е конфигуриран да се ажурира најмалку еднаш дневно и автоматски да ги скенира датотеките во системот/уредот? (Се пополнува ако е избрано А кај А.7.1)

Choose an item.

Ова е обично стандардната поставка за софтвер против малициозен софтвер. Овие поставки можете да ги проверите на екранот за конфигурација за вашиот антивирусен софтвер. Можете да користите кој било антивирусен производ, без оглед дали е бесплатен или платен, сè додека може да ги исполни барањата во ова прашање. За секој случај, Windows Defender е погоден за оваа намена.

А.7.3 (А) Таму каде што имате инсталирано антивирус или друг софтвер за заштита од малвер (МАЛициозен софтВЕР), дали истиот е конфигуриран да ги скенира веб-страниците што ги посетувате и да ве предупредува за пристап до потенцијално штетни веб-страници? (Се пополнува ако е избрано А кај А.7.1)

Choose an item.

Вашиот антивирусен софтвер треба да е интегриран за интернет прелистувачот или за самиот оперативен систем, и на тој начин да спречува пристап до познати штетни веб-страници. На Windows 10, SmartScreen може да ја обезбеди оваа функционалност, во комбинација со интегрираниот антивирусен софтвер Defender или друго комерцијално решение.

А.7.4 (Б) Кога за преземање и инсталација на апликации користите официјални продавници или инсталирате апликации со валиден сертификат и потпис од производителот, дали на корисниците им е оневозможено да инсталираат непотпишани апликации или апликации преземени од сомнителни извори? (Се пополнува ако е избрано Б кај А.7.1)

Choose an item.

Повеќето мобилни телефони и таблети во стандарден режим на користење не дозволуваат да инсталирате непотпишани апликации или апликации од сомнителни извори. Обично треба да се направи т.н. „Рутирање или џеилбрејк“ на уредот за да дозволите инсталирање на непотпишани апликации. Кај компјутерите ограничување се прави преку типот на корисничката сметка која нема привилегии за инсталација на нови апликации.

А.7.5 (Б) Кога за преземање и инсталација користите официјални продавници за апликации или инсталирате апликации со валиден сертификат и потпис од производителот, дали ги ограничувате корисниците да инсталираат апликации само одобрени од вашата организација и дали евиденција/листа на одобрени апликации? (Се пополнува ако е избрано Б кај А.7.1)

Choose an item.

Сајбер одговорна организација треба да поседува список на одобрени апликации, како и да не се дозволи инсталирање на други апликации од страна на вработените на службените уреди и приватните уреди кои се користат за пристап до организациските системи. За да вовоедете вакво ограничување може да користите софтвер за управување со мобилни уреди (Mobile Device Management) и полиси за соодветно кофигурирање на компјутери и лаптопи со што ќе го исполните ова барање. Од вас не се бара задолжително да користите MDM софтвер доколку можете да ги исполните барањата со користење на политика, процес и обука на вработените.

А.7.6 (В) Доколку користите изолација на апликации преку sandoxing, дали обезбедувате забрана овие апликации да пристапат до организациските системи за складирање на податоци, чувствителните документи и надворешни уреди, како и до локалната компјутерска мрежа на организацијата? (Се пополнува ако е избрано В кај А.7.1)

Click or tap here to enter text.

Ако користите виртуелна машина за изолација на апликации со sandboxing, обично можете да ги конфигурирате овие поставки во опциите за конфигурација на софтверот за виртуелизација. Не секоја организација ги користи овие технологии, кои укажуваат на напредна организација која се грижи за сајбер безбедноста.

**Резервна копија од важни податоци**

А.7.7 Дали снимате резервни копии од важните податоци? Опишете како го правите ова.

Click or tap here to enter text.

Една сајбер одговорна организација мора задолжително да има процедура за редовен бекап на важни податоци и системи. При тоа една опција е да го користите т.н. „Правило 1,2,3“, со кое организацијата треба да има 3 копии од важните податоци (првата копија е оригиналот - податоците снимени на уредите што се користа за работа, како и 2 резервни копии) на два различни медиуми (USB или надворешен диск, во облак како Google Drive, Microsoft Azure и сл, или на магнетна лента) со една копија надвор од физичката локацијата за враќање од катастрофи и од примарната физичка локација на организацијата. Честотата на снимање копии од податоците ќе зависи од самата организацијата, но мора задолжително да се прави целосен бекап на податоците во периоди не подолги од 1 месец. Се препорачува дневно и неделно снимање на резервни копии од податоците.

А.7.8 Планови за опоравување од катастрофи и Планови за континуитет во деловното работење. Опишете.

Click or tap here to enter text.

Организацијата мора задолжително да има подготвено, пропишано и периодично да тестира Планови за опоравување од катастрофи (пожар, земјотрес и сл.) и Планови за континуитет на деловното работење. Организацијата мора да и ма дефинирано т.н. време за опоравување и прифатливо време за прекин во работата. Соодветно на овие времиња, потребно е да се прилагодат плановите, и во секој план да се дефинира организацискиот тим кој ќе ги реализира. Повеќе информации и насоки за плановите и ризиците ќе најдете на порталот на MKD-CIRT за обуки: https://lms.mkd-cirt.mk.

**Пријава и справување со сајбер напади и инциденти**

A.7.9 Дали имате воспоставено процес или процедура за пријава на сомнителни пораки, инциденти и активности од страна на вработени? Опишете како се прави ова.

Click or tap here to enter text.

Сајбер одговорна организација мора да има воспоставено процес за пријава на сомнителни активности и инциденти, до дедицирано лице во организацијата кое е одговорно за информациска безбедност, или за ИТ системите на организацијата.

А.7.10 На кој начин ги едуцирате вработените за сајбер заканите на интернет и за користење на добри пракси за сајбер заштита? Опишете како го правите ова.

Click or tap here to enter text.

Сајбер одговорна организација мора да вложува во едукација на своите вработени за значењето на користење добри пракси за сајбер заштита.

**ЗАДОЛЖИТЕЛНО ПРОЧИТАЈТЕ!**

## Согласност

Со пополнување, потпишување и испраќање на овој образец организацијата со назив наведен во поле А.1.1 „Назив на организација“ дава согласност Агенцијата за електронски комуникации да ги снима и обработува податоците од овој документ. Во случај на успешна сертификација на организацијата и добивање на сертификат за „Сајбер одговорна организација“, организацијата е согласна Агенцијата за електронски комуникации на веб-страницата на Националниот центар за одговор на компјутерски инциденти MKD-CIRT како нејзина организациска единица, на адреса <https://mkd-cirt.mk> да ги објави следните податоци:

* Назив на организација (доставен податок од пополнето поле А.1.1 од овој документ);
* Датум на доделување и важност на издаден сертификат и беџ;
* Веб-адреса на организацијата (доставен податок од пополнето поле А.1.5 од овој документ);

## Достава на пополнет образец

Доколку овој документ (пополнет образец) се доставува до Агенцијата за електронски комуникации по е-пошта во електронска форма како додаток на порака, истиот задолжително треба да е потпишан со важечки електронски потпис на одговорно или овластено лице во чиј дигитален сертификат текстот во полето за организација одговара на називот наведен во поле А1.1.1 од овој документ.

Доколку овој документ се доставува до Агенцијата за електронски комуникации по писмен пат во хартија, истиот задолжително треба да е потпишан од овластеното лице на организацијата и излезен печат и архивски број од организацијата, и истиот да се испраќа на адреса:

Национален центар за одговор на компјутерски инциденти

Агенција за електронски комуникации

Кеј Димитар Влахов број 21, 1000 Скопје

## Обработка на пополнет образец и издавање на сертификат и беџ за „Сајбер одговорна организација“.

Агенцијата ќе ги преземе сите мерки што и се на располагање за заштита на доставените документи, информации и податоци како резултат од пополнување или достава на пополнетиот образец – Прашалник за самооценување за сертификациска шема „Сајбер одговорна организација“. Агенцијата за електронски комуникации нема да ги објавува и споделува со други лица податоците и информациите од пополнет образец Прашалник за самооценување за сертификација „Сајбер одговорна организација“, освен тие што се наведени во делот „Согласност“ од овој документ.

## Користење на сертификат и беџ за „Сајбер одговорна организација“

Организацијата на која Агенцијата за електронски комуникации и издала сертификат и беџ за „Сајбер одговорна организација“, има право истите да ги користи и објавува на својата веб-страница со адреса наведена во поле А.1.5 од овој документ, во рок од 12 месеци од издавањето на сертификатот и беџот. Организацијата има право да го користи издадениот беџ во промотивни активности на организацијата во истиот временски период.

Доколку организацијата сака да продолжи со користење на сертификат и беџ, мора повторно да го достави до Агенцијата за електронски комуникации овој пополнет документ по што ќе следи повторно процес на проверка на усогласеност на доставените податоци со барањата наведени во Услови за сертификација за „Сајбер одговорна организација“ објавени на веб страницата на адреса <https://mkd-cirt.mk>.

Организацијата може на свое барање да го прекине користењето на сертификатот и беџот во секое време, со испраќање на писмен допис до Агенцијата за електронски комуникации. Во тој случај, Агенцијата за електронски комуникации во рок од 10 (десет) ќе ги избрише податоците за организацијата од своите системи и од веб страницата <https://mkd-cirt.mk> и за истото ќе ја извести организацијата по писмен пат, на адреса наведена во поле А.1.3 од овој документ

## Сертификат и беџ за „Сајбер одговорна организација“

Агенцијата ќе ја информира организацијата за исполнување на Услови за сертификација за „Сајбер одговорна организација“, ќе и додели и испрати сертификат за сајбер одговорна организација и ќе и дозволи користење на беџ, по претходно извршена проверка од страна на стручната служба, во рок од 10 (десет) дена од прием на овој документ.

Агенцијата за електронски комуникации го задржува правото при обработка на доставените податоци од овој потпишан и испратен документ Прашалник за самооценување, да побара од организацијата дополнителни информации и одговори на прашања и појаснувања, во насока на проверка на точност на доставените податоци и за исполнување на Услови за сертификација за „Сајбер одговорна организација“ објавени на веб-страницата <https://mkd-cirt.mk>.

Доколку при проверката на точноста на доставените податоци од овој документ и/или во случај на неисполнување на Услови за сертификација за „Сајбер одговорна организација“, Агенцијата за електронски комуникации го задржува правото да не и додели на организацијата сертификат и беџ за „Сајбер одговорна организација“.

Во случај на одбивање за издавање на сертификат и беџ за „Сајбер одговорна организација“, организацијата подносител на овој документ има право повторно да достави пополнет образец за Прашалник за самооценување за сертификациска шема „Сајбер одговорна организација“ следејќи ја опишаната процедура објавена на веб-страницата на адреса <https://mkd-cirt.mk>.

Одговорно лице / Потписник. Точноста на внесените податоци во овој образец ги потврдува и Согласноста ја дава одговорното лице:

**Click or tap here to enter text.**

Внеси име, презиме, потпис на одговорното лице.

Внесете Име и Презиме на одговорното лице во организацијата, кое е овластен потписник и со чиј валиден дигитален сертификат треба да е потпишан PDF документот пред да се испрати до MKD-CIRT (Директор, Генерален менаџер...). За испраќање по пошта покрај пофгоре наведеното име и презиме, потребен е потпис од одговорното лице и печат од прганзиаицјата, како и архивски рбој на излезниот документ испратен на адреса:

Национален центар за одговор на компјутерски инциденти MKD-CIRT

Агенција за електронски комуникации

Кеј Димотар Влахов 21, 1000 Скопје