# Минимум сајбер безбедносни стандарди за владините институции

Република Северна Македонија

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Republic of North Macedonia
Ministry of Digital Transformation

DAI
Shaping a more livable world.

TAG International

**Наслов на документот:** Минимум сајбер безбедносни стандарди за владините институции

Историја на документот:

| Датум на објавување | Верзија бр. | Опис |
|---|---|---|
| 26 Јануари 2025 | 5.0 | Петта верзија |


British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product is prepared within the programme Western Balkan Cyber Security funded by the UK Government with the support of the British Embassy Skopje. The content of this publication does not necessarily reflect the position or the opinions of the UK Government.

Овој производ е подготвен во рамки на проектот Сајбер безбедност во Западен Балкан, Рефинансиран од Владата на Обединето Кралство, со поддршка на Британската амбасада Скопје. Мислењата и ставовите наведени во оваа содржина не ги одразуваат секогаш мислењата и ставовите на Британската Влада.

Ky produkt është përgatitur në kuadër të programit Siguria kibernetike në Ballkanin Perëndimor i financuar nga Qeveria e Mbretërisë së Bashkuar me mbështetjen e Ambasadës Britanike Shkup. Përmbajtja e këtij publikimi nuk pasqyron domosdoshmërisht qëndrimin ose mendimet e Qeveria e Mbretërisë së Bashkuar.

## *СОДРЖИНА*

## Предговор

Препознавајќи ја клучната улога на владините институции во безбедноста на чувствителните податоци и критичните услуги, креирана е стандардизирана рамка на сајбер безбедносни стандарди која треба да обезбеди заштита на дигиталните средства, да ја зголеми безбедноста на луѓето, националната безбедност и да овозможи континуитетот на националните есенцијални сервиси. Безбедносните стандарди се креирани од страна на специјална интерресорски група, која обедини владините агенции и претставници од приватниот сектор и академската заедница. Оваа интерресорски група го олесни градењето на доверба, споделувањето на информации и соработката, што доведе до заедничко донесување одлуки и вклучување на различните сектори. Националните експерти ја менторираа групата во развојот, одржувањето и надградувањето на најсовремените стандарди прилагодени на уникатните барања на различни владини институции. Дополнително, креиран е сеопфатен водич кој ќе помогне во разбирањето и ефикасната имплементација на овие стандарди, опфаќајќи анализа на ризици, следење на усогласеност и најдобри практики.

Овие минимални стандарди за сајбер безбедност се состојат од основни побарувања, насоки и практики за сајбер безбедност кои треба да се имплементираат во владините институции на Република Северна Македонија.
Секое поглавје, од 1 до 18, опишува една група на безбедносни контроли. Стандардот содржи побарувања на три нивоа на зрелост во сајбер безбедноста. Изборот и имплементацијата по ниво зависи од големината на организацијата.

- **Ниво 1** е збир на основни побарувања за сајбер безбедност кои треба да бидат имплементирани од сите организации кои првенствено обезбедуваат услуги поддржани од ИКТ системите.
- **Ниво 2** е збир на побарувања за организации кои опслужуваат значителен број граѓани, а услугата е клучна за социјалните и економските фактори на нацијата. Овие побарувања се задолжителни за организации кои обезбедуваат услуга на најмалку 250.000 уникатни корисници.
- **Ниво 3** е збир на напредни побарувања за сајбер безбедност за организации кои се дел од критична инфраструктура, чие не функционирање значително би влијаело на социјалните и економските фактори на нацијата.

Усогласеноста со овие побарувања е неопходна за да се минимизира ризикот од нарушување на функционирањето на владините институции.
Неопходно е да се има во предвид дека сите овие фактори ќе се променат со текот на времето.

| | |
|---|---|
| Забелешка 1 | Владините институции имаат овластување да ги изземат побарувањата кои се технички или организациски невозможно да се имплементираат. Дополнително, ако анализата на ризик утврди дека одредено побарување не е применливо, или ако специфичната цел може да се постигне преку алтернативни безбедносни мерки, тоа побарување може да биде изземено. Оправдувањето за изземање на специфични побарувања е од суштинско значење. |
| Забелешка 2 | Редоследот во кој се појавуваат побарувањата во овој документ не ја означува нивната релативна важност или редоследот по кој треба да се имплементираат. Нумерацијата служи само за полесно референцирање. |
| Забелешка 3 | Побарувањата во овој документ се однесуваат само на владините институции лоцирани на територијата на Република Северна Македонија. |
| Забелешка 4 | Овој стандард се однесува на инфраструктурата (вклучувајќи мрежни уреди, хостови, рутери, средства и др.), софтверот, услугите и податоците кои се во сопственост на владините институции. |

| | |
|---|---|
| Забелешка 5 | Владините институции се советуваат да не ги ограничуваат контролите за спроведување само на нивните доделени нивоа. Наместо тоа, тие треба да се стремат да го спроведат највисокото ниво на безбедносни мерки за подобрување на отпорноста на закани од сајбер просторот. |

## Термини, дефиниции и кратенки

### *Термини и дефиниции*

| Термин | Дефиниција |
|---|---|
| Контрола на пристап | Мерки кои го ограничуваат пристапот до ресурсите само на оние кои за тоа се овластени. |
| Одговорност | Концептот дека поединците се одговорни за своите постапки. |
| Средства | Секој ресурс, уред или информација кои се вредни за организацијата. |
| Автентикација | Процесот на верификација на идентитетот на корисникот, процесот или уредот. |
| Автентичност | Осигурување дека информациите или податоците се вистински и од проверен извор. |
| Достапност | Осигурување дека информациите и ресурсите се достапни за овластените корисници кога е потребно. |
| Континуитет на бизнисот | Способноста на организацијата да продолжи со испорака на производи или услуги на прифатливо претходно дефинирано ниво после одредени сајбер инциденти. |
| Одговорно лице за сигурност за информатичка безбедност (CISO) | Службеник одговорен за воспоставување и одржување на визијата на организацијата, стратегијата и програмата за да се осигура дека информациите се соодветно заштитени. |
| Тим за одговор на инциденти поврзани со компјутерска безбедност (CSIRT) | Тим одговорен за прием, разгледување и одговор на инциденти поврзани со компјутерската безбедност. |
| Комуникациска инфраструктура | Физичките и виртуелните ресурси кои се користат за пренос на податоци, вклучувајќи мрежи, сервери и софтвер. |
| Доверливост | Осигурување дека информациите се достапни само за оние кои се овластени да имаат пристап. |
| Контрола | Заштита или контрамерка за избегнување, откривање, спротивставување или минимизирање на безбедносните ризици. |
| Контрамерки | Активности, уреди, процедури или техники кои ја намалуваат заканата, ранливоста или нападот со елиминирање или спречување. |
| Критична инфраструктура | Витални системи и средства, чие нарушување би имало сериозни последици по националната безбедност, јавната безбедност или економија и кои побаруваат строги мерки за заштита од закани и обезбедување на отпорност. |
| Стратегија за сајбер безбедност | Стратешки документи кои ги опишуваат националните и организациските стратегии за сајбер безбедност, вклучувајќи краткорочни и долгорочни цели. |
| Безбедносна контрола | Специфични мерки или механизми за избегнување на безбедносните ризици. |
| Безбедносни мерки | Различни стратегии и акции преземени за заштита на информациските системи од закани. |
| Информациско средство | Секоја информација или податоци и поврзани системи кои имаат вредност за организацијата. |
| Информациска безбедност | Заштита на информации и информациски системи од неовластен пристап, употреба, откривање, нарушување, модификација или уништување. |

| | |
|---|---|
| Инцидент по информацискатa безбедност | Еден или серија на несакани или неочекувани настани за информациска безбедност кои имаат значителна веројатност за компромитирање на деловните операции. |
| Безбедносни инциденти | Настан кој може да укажува на тоа дека системите или податоците на организацијата се компромитирани. |
| Настан поврзан со информациска безбедност | Идентификувана појава на систем, услуга или мрежна состојба што укажува на можно прекршување на политиките за информациска безбедност или неуспех на заштитата. |
| Систем за управување со информациска безбедност (ISMS) | Систематски пристап за управување со чувствителни информации на компанијата, така што тие остануваат безбедни, вклучувајќи луѓе, процеси и ИТ системи. |
| Политика за информациска безбедност | Збир на правила и практики кои го регулираат начинот на кој организацијата управува, заштитува и дистрибуира информации. |
| ИКТ инфраструктура | Компоненти и системи на информатичката и комуникациската технологија кои се користат за управување и пренесување на информации. |
| Непроменливост на податоците | Осигурување дека информациите се точни и целосни и дека не се изменети на неовластен начин. |
| Внатрешна ревизија | Внатрешни проверки кои се вршат според најдобрите практики, потенцијално од страна на вработени или проверени трети страни, со документација за сите извештаи од ревизиите. |
| Медиуми | Физички или електронски методи за складирање на податоци, вклучувајќи хартија, дискови, УСБ дискови, итн. |
| Nonrepudiation | Конфигурирање на системите и процесите со кои ќе се осигура дека дејствата или настаните се запишани и може да се докажат дека се случиле. |
| Непривилегирана сметка | Корисничка сметка со ограничени права за пристап до системите и податоците. |
| Привилегирана сметка | Сметка со зголемени права за пристап која може да врши административни задачи. |
| Доверливост | Способност на системот или компонентата доследно да ги извршува своите потребни функции под наведени услови за одреден временски период. |
| Ризик | Потенцијалот за загуба или штета поврзана со експлоатација на слабости. |
| Анализа на ризикот | Целокупниот процес на идентификација на ризикот, анализа на ризикот и анализа на ризикот. |
| Анализа на ризикот | Систематска употреба на информации за идентификување и анализа на ризиците за операциите и средствата на организацијата. |
| Закрпа/patch | Ажурирање на софтверот за решавање на проблеми, поправка на грешки или подобрување на функционалноста |

Табела 1 – Термини и дефиниции

### *Кратенки*

| **Кратенка** | |
|---|---|
| API | Апликациски програмски интерфејс (Application Programming Interface) |
| BYOD | Донеси свој уред (Bring Your Own Device) |
| CDP | Континуирана заштита на податоци (Continuous Data Protection) |
| CSIRT | Тим за одговор на инциденти поврзани со компјутерска безбедност (Computer Security Incident Response Team) |
| DAST | Динамичко тестирање на безбедноста на апликации (Dynamic Application Security Testing) |
| DHCP | Динамички протокол за конфигурација на хостови (Dynamic Host Configuration Protocol) |
| DMZ | Демилитаризирана зона (Demilitarized Zone) |
| DNS | Доменски именски систем (Domain Name System) |
| ESP | Обезбедувач на основни услуги (Essential Service Provider) |
| GDPR | Општа регулатива за заштита на податоци (General Data Protection Regulation) |
| HTTP | Протокол за пренос на хипертекст (Hypertext Transfer Protocol) |
| HTTPS | Безбеден протокол за пренос на хипертекст (Hypertext Transfer Protocol Secure) |
| ICT | Информациски и комуникациски технологии (Information and Communications Technology) |
| IDE | Интегрирани развојни окружувања (Integrated Development Environments) |
| IOC | Индикатори за компромитирање (Indicators Of Compromise) |
| IoT | Интернет на нештата (Internet of Things) |
| IPS/IDS | Систем за превенција/откривање на нарушувања (Intrusion Prevention System/Intrusion Detection System) |
| IPX | Интермрежена размена на пакети (Internetwork Packet Exchange) |
| ISAC | Споделување и анализа на информации (Information Sharing and Analysis) |
| ISMS | Систем за управување со информациска безбедност (Information Security Management System) |
| ISP | Политика за информациска безбедност (Information Security Policy) |
| LAN | Локална мрежа (Local Area Network) |
| LLMNR | Решение за мултикаст име на поврзување (Link-Local Multicast Name Resolution) |
| MAC | Контролна адреса на медиум (Media Access Control address) |
| MFA | Повекефакторска автентикација (Multifactor Authentication) |
| NAC | Контрола на пристап до мрежата (Network Access Control) |
| NGFW | Заштитен ѕид со нова генерација (New Generation Firewall) |
| NPI | Нејавна информација (Non-public Information) |
| OSI | Интерконекција на отворени системи (Open Systems Interconnection) |
| OSINT | Разузнувачки информации од отворени извори (Open Source Intelligence) |
| PII | Лични идентификациски информации (Personally Identifiable Information / Personal Data) |
| RDP | Протокол за далечинско работење (Remote Desktop Protocol) |
| RA | Анализа на ризик (Risk Assessment) |

| | |
|---|---|
| SAST | Статичко тестирање на безбедноста на апликации (Static Application Security Testing) |
| SIEM | Систем за управување со безбедносни информации и настани (Security Information and Event Management) |
| SME | Експерти за конкретна тематика (Subject Matter Experts) |
| SOC | Оперативен центар за сајбер безбедност (Security Operation Center) |
| SSH | Протокол за безбедна обвивка (Secure Shell protocol) |
| STIX | Структурирана информација за закани (Structured Threat Information eXpression) |
| TAXII | Trusted Automated eXchange of Indicator Information |
| TLS | Безбедност на транспортен слој (Transport Layer Security) |
| VLAN | Виртуелна локална мрежа (Virtual Local Area Network) |
| VPN | Виртуелна приватна мрежа (Virtual Private Network) |
| WAN | Широка областна мрежа (Wide Area Network) |
| WAF | Веб апликациски оган (Web Application Firewall) |
| WPAD | Протокол за автоматско откривање на веб прокси (Web Proxy Auto-Discovery Protocol) |

# 1. УПРАВУВАЊЕ СО СМЕТКИ И КОНТРОЛА НА ПРИСТАП

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **1.1.** Одржувајте сеопфатен каталог за сите корисници на системот, процеси и уреди.<br>**1.2.** Автентикација на идентитетот на корисниците, процесите и уредите пред да се даде пристап до организациските системи.<br>**1.3.** Ограничете го системскиот пристап исклучиво на овластени корисници, процеси и одобрени уреди, вклучувајќи меѓусебно поврзани системи.<br>**1.4.** Спроведете строги насоки за комплексност на лозинката и задолжителни периодични промени на лозинките.<br>**1.5.** Воспоставете сеопфатна процедура за навремено отстранување на правата за пристап на персоналот кој напуштил или дал оставка.<br>**1.6.** Придржувајте се до принципот на минимална привилегија, доделување на корисниците само специфични безбедносни функции и привилегии потребни за нивните улоги.<br>**1.7.** Спроведете тајмаут на сметката по неколку неуспешни најави.<br>**1.8.** Имплементирајте повеќе-факторски механизми за автентикација за локален и далечински пристап. |
| **2** | **1.9.** Веднаш укинете ги правата за пристап како одговор на злонамерни активности од страна на вработен или добавувач (трета страна), спречувајќи понатамошни неовластени дејства и ограничувајќи го влијанието на нарушувањето на безбедноста.<br>**1.10.** Задолжителна итна промена на лозинката од привремена во постојана по запишување на системот<br>**1.11.** Оневозможете ги неактивни корисници по дефиниран временски период за да се ублажи ризикот од експлоатација на неактивните сметки од страна на неовластени корисници. |
| **3** | **1.12.** Употреба на криптографска заштита за сите зачувани и лозинки во транзит, одржувајќи ја нивната нечитливост дури и ако се пресретнат, со што се подобрува безбедноста против неовластени обиди за пристап.<br>**1.13.** Имплементирајте прикривање/опфускација на повратните информации за автентикација како дополнителна безбедносна мерка, спречувајќи потенцијални напаѓачи да извлечат информации за процесот на автентикација и подобрувајќи ја целокупната безбедносна состојба.<br>**1.14.** Редовна проверка на записи / Следете на успешни најавувања, неуспешни најавувања и заклучени важни/администраторски сметки за откривање на сомнителни активности.<br>**1.15.** **Brake glass account** – административна резервна сметка со највисоки привилегии која се користи во итни случаи |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| *ПРИНЦИП P1.01* | |
|---|---|
| Воспоставување на процедури за безбеден пренос и складирање. | • Идентификувајте доверливи кредентцијали, како што се лозинки, криптографски клучеви и податоци складирани во хардверските токени.<br>• Овозможете уникатност за привремени/пре-дефинирани лозинки, побарувајќи нивна промена после првата употреба. |

| | |
|---|---|
| | • Складирајте само хешови од лозинките, ограничувајќи ги механизмите за преземање на истите користејќи безбедни средини како сефови или безбедносни трезори. |
| Безбедно најавување на критични ИКТ системи | • Прилагодите ги методите за автентикација според природата на системот и чувствителноста на податоците, спроведувајќи анализа на ризик.<br>• Автоматски запишувајте ги сите сесии за далечински пристап, вклучувајќи ги и оние на вработените и надворешниот технички персонал.<br>• Имплементирајте криптографски решенија како VPN, SSH или слични технологии за заштита на преносот на податоци.<br>• Задолжителна употреба на повеќе-факторска автентикација во ИКТ системи што поддржуваат критични процеси за дополнителна безбедност. |
| Ефективни процедури за управување со лозинки | • Наметнете постапка за креирање силни лозинки и задолжителни промени во случај на компромитирање или административна потреба.<br>• Имплементирајте политики за застарување на лозинките за да обезбедите редовни ажурирања и намалување на ризиците од продолжено изложување на истите.<br>• Управувајте со локалните администраторски сметки за да спречите неовластен пристап и злоупотреба.<br>• Елиминирајте потенцијални безбедносни ранливости преку управување со вградените локални администраторски сметки во оперативните системи.<br>• Користете менаџери за лозинки или хардверски криптирани УСБ уреди за системи што не се покриени од директориум услугите. |
| ***ПРИНЦИП P1.02*** | |
| Редовен преглед на пристапните записи за привилегирани сметки | • Спроведувајте редовен преглед на пристапните записи за привилегирани сметки со цел идентификување и документирање на абнормални однесувања.<br>• Користете проактивно мониторирање за да откриете и ублажите потенцијални обиди за неовластен пристап.<br>• Користете аларми во случај на нерегуларна употреба на привилегирана сметка. |
| Имплементација на Централизирано Решење за Управување со Пристап | • Имплементирајте централизирано решение за управување и контрола на пристап до критични системи и ресурси.<br>• Наметнете јаки механизми за автентикација, авторизација и ревизија за привилегирани сметки. |
| ***ПРИНЦИП P1.03*** | |
| Воспоставување на Постапки за Доделување Кориснички Овластувања | • Воспоставете постапки за доделување, измена, одземање и регистрирање на кориснички овластувања.<br>• Одржувајте ажурирана документација за правата на пристап на корисниците и веднаш отстрани или ажурирај пристапни привилегии како одговор на промените. |

| | |
|---|---|
| Уникатни Кориснички Идентификатори | • Доделете уникатни идентификатори за воспоставување одговорност и следење во ИКТ системот.<br>• Периодично проверувајте и бришете или блокирајте неискористени идентификатори, осигурувајќи дека секој идентификатор е доделен само еднаш. |
| Овластувања и Барања за Пристап | • Овластете пристап до ИКТ системите само по одобрување на барањата за пристап.<br>• Веднаш одземете или ажурирајте го пристапот кога ќе се сменат улогите или кога корисниците ќе ја напуштат организацијата. |
| ***ПРИНЦИП P1.04*** | |
| Ограничување на Неуспешни Обиди за Најава | • Дефинирајте го бројот на неуспешни обиди за најава врз основа на барањата на системот/апликацијата.<br>• Подобрете ја безбедноста со ограничување на неуспешните обиди за најава на препорачаните вредности. |
| Идентификација и Ограничување на Привилегиран Пристап | • Идентификувајте ги привилегираните права на пристап по систем или процес, ограничувајќи го пристапот на неопходниот минимум за извршување на задачите.<br>• Внимателно контролирајте ги администраторските права на оперативни системи, бази на податоци и апликации. |
| Редовен Преглед на Администраторски Права | • Квартално прегледувајте и проверувајте ги администраторските права, осигурувајќи правилна контрола на пристапот.<br>• Извршувајте прегледи најмалку на секои 6 месеци, или почесто ако е потребно за да се усогласи со барањата на организацијата. |

## 2. КОНТРОЛА НА КАТАЛОГ НА СРЕДСТВА (ХАРДВЕР И СОФТВЕР)

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **2.1.** Воспоставете сеопфатен каталог на сите средства кои складираат или обработуваат податоци, вклучувајќи важни детали како мрежна адреса, хардверска адреса и статус на одобрување на одредена централна локација.<br>**2.2.** Воспоставете детален каталог кој ги покрива средствата поврзани физички, виртуелно, од далечина и во облак околини, дури и ако не се директно контролирани.<br>**2.3.** Воспоставете детален каталог на целиот лиценциран софтвер инсталиран на деловните средства, документирајте важни информации за софтверот.<br>**2.4.** Имплементирајте основни постапки за идентификација на неовластен софтвер и преземете соодветни мерки. |
| **2** | **2.5.** Започнете со имплементација на технички контроли како што е дозволеното извршување на апликации за да се овозможи само стартување на авторизирани софтвери.<br>**2.6.** Зајакнете ги практиките за документација за да вклучуваат сеопфатни детали како што се спецификациите на средствата, информации за конфигурација и инсталиран софтвер.<br>**2.7.** Интегрирајте ги со постоечките системи за управувањето со ИТ за да ја зголемите ефикасноста и точноста во следењето и управувањето со средствата низ целата организација.<br>**2.8.** Дефинирајте јасни улоги и одговорности за одржување на каталогот на софтверот меѓу персоналот, осигурувајќи одговорност и конзистентност. |
| **3** | **2.9.** Користете алатки за активно и пасивно откривање за да ги идентификувате средствата поврзани со мрежната инфраструктура, осигурувајќи целосна покриеност.<br>**2.10.** Одржувајте неделна процедура за откривање и управување со неовластени средства во рамките на мрежната инфраструктура.<br>**2.11.** Имплементирајте автоматизација и механизми за следење во реално време за да го олесните откривањето на средства, ажурирањето на каталогот и промените на статусот, осигурувајќи ефикасност и точност.<br>**2.12.** Навремено преземете неопходни акции при идентификација на неовластени средства, како што се отстранување, одбивање на далечински пристап или карантин, за ефикасно да се намалат потенцијалните ризици,<br>**2.13.** Конфигурирајте алатката за активно откривање да се извршува дневно и редовно прегледувајте ги пасивните скенирања за да го ажурирате каталогот на средствата, осигурувајќи негова точност и целосност на неделна основа. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***ПРИНЦИП P2.01*** | |
|---|---|
| Сеопфатно преглед на каталог | • Составете сеопфатен преглед на каталог за сите средства кои имаат способност за складирање или обработка на податоци.<br>• Зачувајте ги основните детали како мрежна адреса, хардверска адреса, име на машината, сопственик на средството, оддел и статус на одобрување за мрежно поврзување. |
| Зајакнување на документацијата | • Зајакнете ги практиките за документација за да вклучуваат сеопфатни детали, како што се спецификациите на средствата, информации за конфигурација и инсталиран софтвер.<br>• Интегрирајте ги со постоечките системи за управување со ИТ за да ја зголемите ефикасноста и точноста во следењето и управувањето со средствата. |
| Неделно откривање и управување со неовластени средства | • Употребувајте неделна процедура за откривање и управување со неовластени средства во рамките на мрежната инфраструктура.<br>• Навремено преземете неопходни акции, како што се отстранување, одбивање на далечински пристап или карантин, за да ги ублажите потенцијалните ризици. |
| ***ПРИНЦИП P2.02*** | |
| Распоредување на активни и пасивни алатки за откривање | • Користете алатки за активно и пасивно откривање за да ги идентификувате средствата поврзани на мрежната инфраструктура.<br>• Конфигурирајте ја алатката за активно откривање да се извршува секојдневно, додека DHCP запишувањето се проверува и користи за да го ажурира каталогот на средствата на неделна база. |
| Редовни прегледи за ажурирање на каталогот | • Спроведувајте редовни прегледи на пасивните скенирања за да го ажурирате каталогот на средствата, осигурувајќи точност и целосност.<br>• Прегледувајте ги пасивните скенирања најмалку еднаш неделно за да одржите ажуриран каталог на мрежните средства. |
| ***ПРИНЦИП P2.03*** | |
| Воспоставување на сеопфатен каталог на софтвер | • Започнете со процесот на воспоставување сеопфатен каталог на целиот лиценциран софтвер инсталиран на средствата.<br>• Документирајте ги основните информации за секој софтвер, вклучувајќи наслов, издавач, датум на иницијална инсталација/користење и намена. |
| Идентификација и управување на неавторизиран софтвер | • Воспоставете процедури за идентификување на неовластен софтвер на средствата на организацијата.<br>• Преземете соодветни акции за справување со неовластен софтвер, спроведувајќи прегледи месечно или почесто, доколку е потребно. |

| | |
|---|---|
| Имплементација на дозволената листа на апликации | • Започнете со имплементација на технички контроли, како што е дозволени листи на апликации (allowlisting), за да ја подобрите безбедноста.<br>• Редовно прегледувајте и ажурирајте ги политиките што го регулираат вчитувањето на софтверските библиотеки за да се приспособат на промените во системските барања и најдобрите безбедносни практики. |
| Контрола на вчитувањето на софтверските библиотеки | • Воспоставете политики за да ги специфицирате одобрените библиотеки кои имаат дозвола да се вчитуваат во системските процеси.<br>• Имплементирајте автоматизирани алатки или скрипти за да го забрзате собирањето на податоци и ажурирањата во каталогот на софтверот. |
| Дефинирање на улоги и одржување | • Дефинирајте улоги и одговорности за одржување на листата со софтверски каталогот за персоналот.<br>• Спроведувајте редовно одржување и ажурирање на алатките за каталог на софтвер за да се осигури оптимална работа и непроменливост на податоците. |

## 3. БЕЗБЕДОСНА КОНФИГУРАЦИЈА И УПРАВУВАЊЕ СО ЗАКРПИ (СРЕДСТВА)

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **3.1.** Користете ги способности на вградениот заштитен sид од оперативниот систем на серверот за да го ограничите влезниот и излезниот мрежен сообраќај врз основа на однапред дефинирани правила.<br>**3.2.** Редовно прегледувајте и ажурирајте ги правилата за заштитен sид за да се усогласат со безбедносните политики и барања на организацијата, прилагодувајќи ги на развојот на заканите и потребите.<br>**3.3.** Овозможете записи на активностите на заштитен sид и редовно следете ги записите за било какви сомнителни или неовластени обиди за пристап, овозможувајќи навремено откривање и одговор на потенцијални безбедносни нарушувања.<br>**3.4.** Веднаш променете ги предефинираните лозинки на сметките за да се намали ризикот од неовластен пристап.<br>**3.5.** Одржувајте документација со детали за предефинираните сметки и лозинки и осигурете се дека релевантниот персонал е свесен за важноста од промена на овие стандардни поставки при извршување, за да се подобри безбедносната свесност и усогласеност.<br>***3.6.*** Оневозможете ги предефинираните сметки кои не се потребни за работа на системот или административни задачи за да спречите потенцијална злоупотреба или експлоатација, зајакнувајќи ја безбедноста на сметките. |
| **2** | **3.7.** Распоредете соодветно решение за заштитен sид за да обезбедите напредни безбедносни функции за мрежата, како што се филтрирање на ниво на апликација и откривање на нарушувања.<br>**3.8.** Имплементирајте сегментација на мрежата користејќи го заштитен sид за да ја поделите серверската околина на одделни зони врз основа на нивоата на доверба, со цел да го ограничите и ублажите влијанието на безбедносните нарушувања.<br>**3.9.** Имплементирајте Контрола на Пристап базирана на Улоги (RBAC): Доделете привилегии и права на пристап врз основа на работни улоги за да го ограничите пристапот до критични функции и податоци, подобрувајќи ја безбедноста и минимизирајќи го ризикот од неовластен пристап. |
| **3** | **3.10.** Инсталирајте и конфигурирајте агент за заштитен sид од трета страна на секој сервер за да ја зајакнете безбедноста преку додавање на дополнителни слоеви на заштита покрај основниот заштитен sид на оперативниот систем.<br>**3.11.** Имплементирајте континуирано следење на усогласеноста за да осигурете дека конфигурациите на заштитен sид остануваат усогласени со индустриските стандарди и регулаторните барања, одржувајќи ги најдобрите безбедносни практики.<br>**3.12.** Имплементирајте решенија за откривање на било какви неовластени обиди за пристап до предефинирани сметки или промени на конфигурациите на предефинирани сметки во реално време, овозможувајќи брз одговор на потенцијални безбедносни инциденти. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***ПРИНЦИП P3.01*** | |
|---|---|
| Користење на вградениот заштитен sид од оперативниот систем | • Искористете го вградениот заштитен sид од оперативниот систем (На пример. Windows заштитен sид, iptables) за да го регулирате влезниот и излезниот мрежен сообраќај врз основа на однапред дефинирани правила.<br>• Имплементирајте правила за контрола на пристапот до одредени портови и протоколи, минимизирајќи ја површината на напад. |
| Редовен Преглед и Ажурирање | • Редовно прегледувајте и ажурирајте ги правилата на заштитен sид за да се осигурите дека се усогласени со безбедносните политики и барања на организацијата.<br>• Спроведувајте периодични ревизии за да ги идентификувате и отстраните непотребните или застарените правила, оптимизирајќи ја работата и ефикасноста на заштитен sид. |
| Запишување и мониторирање | • Овозможете запишување на активностите на заштитен sид и воспоставете процеси за редовно следење на записите за да откриете сомнителни или неовластени обиди за пристап.<br>• Имплементирајте механизми за алармирање за да го известите безбедносниот персонал за потенцијални безбедносни инциденти или прекршувања на политиките во реално време. |
| ***ПРИНЦИП P3.02*** | |
| Мерки за безбедност на сметки | • Имплементирајте мерки како политики за силни лозинки, повеќе факторска автентикација (MFA) и механизми за заклучување на сметките за да ги заштитите од неовластен пристап, намалувајќи го ризикот од напади базирани на кредендцијали.<br>• Веднаш променете ги предефинираните лозинки за сметки како „root“, „administrator“ или било која друга однапред конфигурирана сметка од добавувачот при воведување на средството или софтверот.<br>• Користете силни и уникатни лозинки за да спречите неовластен пристап и потенцијална експлоатација на кредендцијалите од основните сметки. |
| Документации и свесност | • Одржувајте сеопфатна документација со детали за основните сметки и нивните лозинки, осигурувајќи дека релевантниот персонал е свесен за важноста од промена на овие поставки.<br>• Обезбедете обуки и сесии за подигнување на свеста за да ги едуцирате администраторите и корисниците за ризиците поврзани со основните сметки и важноста на добрата практика за лозинки. |
| Редовна Ревизија и Спроведување | • Спроведувајте редовни ревизии за да ги идентификувате сите инстанци каде што предефинираните сметки не се променети и навремено преземете корективни мерки.<br>• Имплементирајте автоматизирани механизми за спроведување на усогласеност со политиките за промена |

| | |
|---|---|
| | на лозинки и намалување на ризикот од неовластен пристап. |
| ***ПРИНЦИП P3.03*** | |
| Напредни Безбедносни Функции за Мрежа | • Распоредете решенија за заштитен sид за да обезбедите напредни безбедносни функции за мрежата, вклучувајќи филтрирање на ниво на апликации, откривање на нарушувања и поддршка за VPN.<br>• Искористете ги овие функции за да ја подобрите целокупната безбедносна состојба на организацијата и да се заштитите од постојаната еволуција на сајбер заканите. |
| Сегментација на мрежа | • Имплементирајте сегментација на мрежата користејќи заштитен sид за да ја поделите серверската околина на одделни зони врз основа на нивоа на доверба (на пример, DMZ, внатрешна мрежа).<br>• Изолирајте ги критичните компоненти на инфраструктурата од помалку безбедните области за да го ограничите и ублажите влијанието на безбедносните закани и обиди за неовластен пристап. |
| Интеграција со Безбедносна Автоматизација | • Интегрирајте огнени sид со алатки за автоматизација на безбедноста за да ги автоматизирате одговорите на откриени закани, како што е блокирање на малициозни интернет адреси или активирање на аларми за понатамошна истрага.<br>• Поедноставете ги процесите за одговор на инциденти и подобрете ја способноста на организацијата да открие и ублажи безбедносни инциденти во реално време. |

## 4. УПРАВУВАЊЕ СО РАНЛИВОСТИ И ПЕНЕТРАЦИСКО ТЕСТИРАЊЕ

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **4.1.** Воспоставете процес за управување со ранливостите на средствата.<br>**4.2.** Периодична анализа на организациските системи за да се утврди дали безбедносните контроли се ефективни при нивната примена.<br>**4.3.** Програма за пенетрациско тестирање интегрирана во поширокатa рамка за одговор на инциденти. - Потребно е редовно пенетрациско тестирање, најмалку еднаш во две години или по значителни промени или воведување нови системи.<br>**4.4.** Воспоставете процес на управување со закрпи. |
| **2** | **4.5.** Воспоставете процедури и алатки за справување со детектираните ранливости на софтверот на месечно ниво, по што ќе воспоставите процедури за справување со ранливостите врз основа на нивото на ранливост.<br>**4.6.** Воспоставете периодично скенирање на ранливости во организациските ИКТ системи и апликации, како и во ситуации кога ќе се идентификуваат нови пропусти што влијаат на тие системи и апликации. |
| **3** | **4.7.** Креирајте посебен тим за пенетрациско тестирање (црвен тим) за да се изврши пенетрациско тестирање на системот или системските компоненти.<br>**4.8.** Автоматизирајте ги скенирањата на ранливостите на квартална основа на надворешно изложените средства, користејќи алатки за скенирање на ранливости.<br>**4.9.** Воспоставете процес на пенетрациско тестирање кој опфаќа обиди да се запрат или заобиколат контролите поврзани со физичките пристапни точки до објектите. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| *ПРИНЦИП П4.01* | |
|---|---|
| Следете и добивајте информации за техничките ранливости на ИКТ системите кои се користат на тековна основа и проценете ја изложеноста на организацијата на нив, како и преземете соодветни мерки за да се спротивставите на поврзаниот ризик(и) | • Воспоставете регистар на идентификувани ИКТ ресурси кои поддржуваат критични услуги кој е предуслов за управување со ранливости.<br>• Критични ажурирања и конфигурациски промени (откако ќе се потврди дека се без грешки) треба да се воведат веднаш по нивното објавување.<br>• Користете апликации од најновата можна верзија и вршете редовно ажурирање. Ова особено се однесува на веб-прелистувачи, Microsoft Office и читачи на PDF. Од моментот на нивното објавување (и потврдата дека тие се без грешки), закрпи/корекции/ажурирање на апликациите одговорни за поддршка на критичните процеси спроведени од операторот треба да се инсталираат без непотребно одлагање.<br>• Оперативните системи и мрежните уреди треба да се користат во ажурирана верзија. Не се препорачува да се користат верзии кои повеќе не се поддржани. Од моментот на нивното објавување (и потврдата дека тие се без грешки), закрпи/корекција/ажурирање на |

| | |
|---|---|
| | оперативните системи и мрежните уреди одговорни за поддршка на критичните процеси спроведени од операторот треба да се инсталираат без непотребно одложување. |
| Управувањето со техничките пропусти бара конкретни информации, како што се | • податоци за провајдерот на софтвер,<br>• број на верзија,<br>• на кој систем е инсталиран софтверот,<br>• времетраењето на техничката поддршка и лиценците на производителот на софтверот.<br>• Информации за ранливости и закани може да се добијат од тимови за одговор на компјутерски инциденти, на пр., MKD-CIRT и владин CIRT |
| ***ПРИНЦИП П4.02*** | |
| Редовен - двегодишен распоред за пенетрациско тестирање и усогласеност | • Поставете конзистентен распоред за спроведување на годишно пенетрациско тестирање од надворешна независна компанија.<br>• Усогласете го распоредот со организациските цели, барањата за усогласеност и најдобрите практики во организацијата.<br>• Создадете процедури за справување со откриените пропусти. |
| Следете ја усогласеноста | • Воведете механизми за следење на усогласеноста со годишниот распоред за пенетрациско тестирање.<br>• Користете автоматски потсетници, алатки за следење на напредокот или периодични прегледи од безбедносни структури.<br>• Редовно оценувајте го придржувањето до распоредот и преземајте корективни активности по потреба за да обезбедите навремени и планирани активности за пенетрациско тестирање. |
| ***ПРИНЦИП П4.03*** | |
| Структуриран и документиран пристап за да се идентификуваат, проценат, да им се даде приоритет и да се намалат ранливостите на сите средства во рамките на инфраструктурата на организацијата | • Развијте сеопфатна рамка која содржи чекори за управување со ранливости, вклучително идентификација, анализа, приоретизирање и избегнување. Осигурете се дека оваа рамка е добро документирана и лесно достапна за релевантниот персонал.<br>• Закажете рутинска анализа на ранливостите, користејќи ги алатките за автоматско скенирање и рачните методи. Погрижете се овие проценки да ги покриваат сите средства во рамките на инфраструктурата на организацијата и да се спроведуваат редовно за да се идентификуваат новите ранливости и промени во ризиците. |
| Јасна процедура која го опишува процесот на управување со ранливостите за средствата | • Направете детален документ за процедурата што го опишува пристапот на организацијата кон управувањето со ранливостите, вклучувајќи ги улогите и одговорностите, процедурите за анализа, критериумите за одредување приоритети и стратегиите за избегнување. Погрижете се оваа процедура да се прегледува редовно и да се ажурира по потреба за да ги |

| | |
|---|---|
| | одрази промените во технологијата или организациските барања.<br>• Кога процедурата е финализирана, ефикасно споделете ја со сите релевантни чинители во организацијата. Обезбедете обука и ресурси за да се осигурите дека вработените ги разбираат нивните улоги и одговорности во процесот на управување со ранливоста и се свесни за важноста на придржувањето кон насоките на процедурата. |
| ***ПРИНЦИП П4.04*** | |
| Класифицирајте ги средствата, применувајте приспособени контроли за пристап, автоматизирајте ги скенирањата за ранливост за сеопфатно избегнување на ризикот | • Оценете го секое средство во рамките на инфраструктурата на организацијата за да ја одредите неговата критичност и важност. Класифицирајте ги средствата во различни категории врз основа на фактори како што се нивната вредност, чувствителност и влијание врз организациските цели.<br>• Кога средствата ќе се класифицираат, спроведете контроли на пристап и безбедносни мерки прилагодени на нивните соодветни класификации. Ограничете го пристапот до клучните средства само на овластен персонал и спроведете построги безбедносни мерки за да ги заштитите чувствителните или средствата со висока вредност од неовластен пристап или манипулација. |
| Автоматизирани алатки за скенирање на ранливости за постојано следење на средствата за ранливости | • Изберете и распоредете автоматизирани алатки за скенирање на ранливости способни за скенирање и идентификување на ранливости во сите средства во инфраструктурата на организацијата. Конфигурирајте ги овие алатки за да вршат редовни скенирања и да генерираат извештаи со детали за идентификуваните пропусти и поврзаните ризици.<br>• Интегрирајте ги алатките за скенирање со каталог на средства: интегрирајте ги алатките за скенирање на ранливости со системот за попис на средства на организацијата за да се обезбеди сеопфатна покриеност и видливост. Автоматски ажурирајте ги записите за залиха на средства врз основа на резултатите од скенирањето, овозможувајќи прецизно следење на пропустите и нивните поврзани средства. |
| Редовни скенирања за сеопфатна покриеност | • Дефинирајте редовен распоред за скенирање на ранливост врз основа на профилот на ризик на организацијата, оперативните барања и обврските за усогласеност. Погрижете се скенирањето да се врши доволно често за да се обезбеди навремен увид во положбата на ранливоста на организацијата без да се предизвика непотребно нарушување на деловните операции.<br>• Покрај редовните скенирања, воведете скенирање како одговор на значајни промени во инфраструктурата на организацијата, како што се ажурирања на системот, нови распоредувања или безбедносни инциденти. Овие насочени скенирања помагаат да се осигура дека |

| | |
|---|---|
| | ранливостите се навремено идентификувани и адресирани кога ќе се појават. |
| ***ПРИНЦИП П4.05*** | |
| Редовни проценки на ризик за да се оцени потенцијалното влијание на идентификуваните ранливости | • Проценете го потенцијалното влијание на идентификуваните пропусти врз средствата, системите и операциите на организацијата. Користете методологии и алатки за анализа на ризик за да ја анализирате веројатноста и сериозноста на експлоатацијата, земајќи ги предвид факторите како што се критичноста на средствата, векторите на напад и постоечките безбедносни контроли.<br>• Дадете приоритет на ранливостите за отстранување врз основа на нивните оценки за ризик, фокусирајќи се на оние со најголема веројатност и потенцијално влијание од експлоатација. Најпрво, доделете ресурси и внимание на решавање на критичните ранливости, а потоа на оние со пониски нивоа на ризик, за да ја максимизирате ефективноста на напорите за избегнување. |
| Приоритет на ранливостите врз основа на сериозноста и потенцијалното влијание | • Дефинирајте збир на критериуми за анализа на сериозноста на ранливостите, земајќи ги предвид факторите како што се експлоатибилноста, влијанието и засегнатите средства. Развијте систем за бодување или скала за рангирање на ранливостите врз основа на нивните нивоа на сериозност, кои се движат од ниски до критични. |
| ***ПРИНЦИП П4.06*** | |
| Процедури за навремена примена на безбедносни закрпи и ажурирања за избегнување на идентификуваните пропусти | • Создадете документирани процедури за идентификување, тестирање и распоредување безбедносни закрпи и ажурирања низ инфраструктурата на организацијата.<br>• Дефинирајте ги улогите и одговорностите за секој чекор од процесот на управување со закрпи, обезбедувајќи јасна одговорност и координација. |
| Процес за тестирање закрпи пред распоредувањето за да ги минимизирате прекините | • Создадете посветено опкружување за тестирање каде што ќе може безбедно да се распоредат и евалуираат закрпи пред да бидат пуштени во производствени системи. Клонирајте ја производната средина на организацијата што е можно поблиску за да се осигурете дека резултатите од тестирањето точно ги одразуваат условите во реалниот свет.<br>• Тестирајте ги закрпите за компатибилност со постоечките системи, апликации и конфигурации за да ги идентификувате потенцијалните конфликти или проблеми што би можеле да настанат по распоредувањето. Направете регресивно тестирање за да потврдите дека закрпите не воведуваат нови пропусти или несакани последици. |

| | |
|---|---|
| Процедури за реагирање и отстранување на критичните пропусти | • Дефинирајте процедури за ескалација за критичните пропусти кои бараат итно внимание или санација. Воспоставете критериуми за зголемување на ранливостите на повисокото раководство или извршното раководство за приоритетни активности и распределба на ресурси.<br>• Воспоставете протоколи за итно поправање за критичните пропусти кои претставуваат непосредна закана за безбедноста или операциите на организацијата. Развијте процедури за забрзано тестирање на закрпи, одобрување и распоредување за да се минимизира прозорецот на изложеност и да се намали ризикот од експлоатација. |
| Редовни извештаи за положбата на ранливоста на организацијата и напредокот во санирањето | • Создавајте редовни извештаи кои ги сумираат позициите на ранливоста на организацијата, вклучувајќи го бројот на идентификувани ранливости, нивните нивоа на сериозност и статусот на напорите за санација. Приспособете ги извештаите за да ги задоволат потребите на различни засегнати страни, обезбедувајќи релевантни сознанија и метрика за поддршка на донесувањето одлуки и приоритизацијата.<br>• Дистрибуирајте ги извештаите за управување со ранливоста до релевантните засегнати страни во организацијата, вклучувајќи го извршното раководство, управувањето со ИТ и безбедносните тимови. Закажете редовни состаноци или презентации за да разговарате за наодите од извештаите, да ги решите проблемите и да го следите напредокот кон целите за санација на ранливоста. |

## 5. УПРАВУВАЊЕ И РЕВИЗИЈА НА ЗАПИСИ

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **5.1** Идентификувајте ги видовите настани што системот може да ги запише како поддршка на процесот на ревизија.<br>**5.2** Дефинирајте го процесот за управување со ревизорските записи, вклучувајќи ги барањата за прибирање, преглед и зачувување на записите за средства што ќе овозможат следење, анализа, истрага и известување за незаконски или неовластени активности во системот.<br>**5.3** Дејствата на поединечните корисници на системот може уникатно да се поврзуваат со тие корисници, така што тие можат да бидат одговорни за своите постапки.<br>***5.4*** Редовно прегледување и ажурирање на типовите настани избрани за записи. |
| **2** | **5.5** Постојан преглед на релевантните запишани настани.<br>**5.6** Способност на системот да ги споредува и синхронизира внатрешните системски часовници со авторитетен извор за да генерира временски записи за ревизија.<br>**5.7** Заштитете ги информациите за ревизија и алатките за запишување на неовластен пристап, модификација и бришење.<br>**5.8** Инкорпорирајте алатки за автоматско прибирање и анализа на податоците од мониторирање и записите.<br>***5.9*** Приберете записи од провајдерот, каде што има поддршка, вклучувајќи настани како автентикација и авторизација, создавање и отстранување податоци и управување со корисници. |
| **3** | **5.10** Ревизорските записи постојано се прибираат од сите средства.<br>**5.11** Ограничете го управувањето на ревизорските записи на мала група на привилегирани корисници.<br>***5.12*** Дефинирајте аларм и одговор на неуспеси во процесот на прибирање на записи. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***ПРИНЦИП П5.01*** | |
|---|---|
| Идентификувајте ги видовите настани што системот може да ги запише | • Составете листа на сите настани што моментално се евидентирани од системот (на пр., записи за пристап, промени во конфигурацијата, безбедносни предупредувања).<br>• Споредете ги постоечките записи со индустриските стандарди и регулаторните барања за да се идентификуваат записите што недостасуваат.<br>• Прилагодете ги системските поставки или интегрирајте нови алатки за зачувување на потребните настани.<br>• Тестирајте го ажурираниот систем за да потврдите дека точно ги евидентира новите настани.<br>• Кога е потребно, прегледајте ги можностите за евиденција за да се прилагодат на новите закани и регулаторни промени. |
| ***ПРИНЦИП П5.02*** | |
| Ревизорските записи треба да | • Треба да се имплементира систем за запишување на настани во мрежи и ИКТ системи. |

| | |
|---|---|
| ги исполнуваат следново | • Процедурите за архивирање на собраните записи треба да се развијат за период од најмалку 12 месеци и во согласност со GDPR и/или организациски барања. |
| Дневникот на настани треба да содржи збир на минимални информации, вклучувајќи | • Уникатен кориснички идентификатор,<br>• датум, време и детали за клучните настани, на пр., временски ознаки на системски настани вклучувајќи успешни и неуспешни обиди за најавување,<br>• промени во системската конфигурација,<br>• користење на привилегии,<br>• промени на привилегии,<br>• употреба на избрани системски алатки и апликации,<br>• мрежни адреси,<br>• аларми креирани од системот за контрола на пристап,<br>• активирање и деактивирање на системи за заштита, на пр., антивирусен софтвер. |
| Системските администратори не треба да бидат овластени да бришат модифицирани или деактивирани записите за ревизија | • оние кои содржат записи за нивните сопствени активности или клучни настани во системот<br>• за системи каде што тоа е невозможно, треба да се обезбеди механизам за копирање во надворешно складиште како што се сервери за евиденција за ревизија или SIEM системи<br>• Онаму каде што се прават модификации на дневниците (на пример да се отстранат PII или други податоци во согласност со GDPR или други законски барања), оваа активност исто така мора да може целосно да се ревидира, со записи и настани, а таквата активност треба да биде поткрепена со формална организациска политика и процес на одобрување. |
| Онаму каде што е пропорционално и се смета за неопходно, организацијата треба да го прошири опсегот на запишаните настани. | • Проширувањето на запишаните настани го подобрува безбедносниот мониторинг, обезбедува усогласеност, го подобрува управувањето со ризикот, помага одговорот на инцидентот, ја олеснува форензичката анализа и овозможува евалуација на перформансите. |
| ***ПРИНЦИП П5.03*** | |
| Воспоставете периодичен процес на преглед и анализа на ревизорските записи и записи за да се идентификуваат трендовите, аномалиите или потенцијалните | • Развивање распоред за редовно прегледување на записите и доделување одговорност на одреден персонал.<br>• Воспоставување критериуми за идентификација на сомнителни или невообичаени активности во записите.<br>• Имплементирање на автоматизирани алатки или процеси за помош при анализа на записите и идентификација на потенцијални проблеми. |

| | |
|---|---|
| безбедносни инциденти. | |
| ***ПРИНЦИП П5.04*** | |
| SIEM алатките или еквивалентни системи може да се користат за складирање, корелација, нормализирање и анализа на информациите од записите и за генерирање на предупредувања. | • Имајте јасно разбирање за шемите за податоци, библиотеките на средствата за податоци и другите извори на записи.<br>• Направете A/B тестирање за правилата и предупредувањата за основање и подесување.<br>• Избегнувајте „тврдо кодирани“ правила каде што е можно.<br>• Документирајте ги случаите за употреба и клучни индикатори за мерење на перформанси за евалуација и ефикасност.<br>• Обезбедете секакви алатки и предупредувања да ја заштитат доверливоста, интегритетот и достапноста на складираните записи.<br>• Осигурајте се дека се воспоставени и дефинирани соодветните политики за складирање, задржување и предупредување.<br>• Осигурајте се дека целиот релевантен персонал има соодветна обука и дека се одржуваат нивоата на обука. |
| ***ПРИНЦИП П5.05*** | |
| Обезбедете точност на изворите на времето и избегнувајте промена на часовникот | • Конфигурирајте најмалку два синхронизирани извори на време низ средствата на институцијата<br>• Каде што е можно, размислете за користење добро воспоставени извори (на пр. временски сервери на pool.ntp.org) |

## 6. ЗАШТИТА НА Е-ПОШТА И ПРЕЛИСТУВАЧИ

| НИВО | БЕЗБЕДНОСНИ МЕРКИ |
|---|---|
| 1 | **6.1** Воспоставете политика со која се задолжува употребата на само целосно поддржани прелистувачи и клиенти за е-пошта во рамките на организацијата, обезбедувајќи компатибилност и безбедност.<br>**6.2** Имплементирајте DNS услуги за филтрирање на сите средства во организацијата за да го блокирате пристапот до познатите малициозни домени, подобрувајќи ја севкупната мрежна безбедност.<br>**6.3** Спроведете попис на сите додатоци за прелистувачи и клиенти за е-пошта, екстензии и додатоци инсталирани во организацијата.<br>**6.4** Конфигурирајте ги основните правила на главната порта за е-пошта за да ги блокирате влезните е-пораки што содржат специфични екстензии на датотеки за дадени прилози, намалувајќи ја веројатноста за инфилтрација на злонамерен софтвер преку каналите за е-пошта. |
| 2 | **6.5** Користете групни политики или алатки за управување за да се наметне усогласеност со политиките, обезбедувајќи доследна примена кај сите уреди и корисници.<br>**6.6** Воспоставете јасни политики и упатства во врска со инсталирањето и користењето на додатоци за прелистувачи и клиентите за е-пошта, екстензии и додатоци, минимизирајќи го ризикот од воведување на ранливости или неовластен софтвер. |
| 3 | **6.7** Воведете контроли за да спречите извршување на не-поддржани прелистувачи и клиенти за е-пошта во рамките на мрежата на организацијата, намалувајќи ги безбедносните ризици поврзани со застарен или ранлив софтвер.<br>**6.8** Користете групни политики или алатки за управување со конфигурации за да го наметнете усогласеност со политиките, обезбедувајќи доследна примена кај сите уреди и корисници.<br>**6.9** Приспособете ги правилата за DNS филтрирање врз основа на специфичните потреби и профилот на ризик на организацијата, оптимизирајќи ја заштитата од малициозни домени и закани.<br>**6.10** Подобрете ја заштитата на серверот за е-пошта против злонамерен софтвер со напредни техники за откривање, како што се хеуристичка анализа и следење на однесувањето, подобрување на откривањето и избегнувањето на софистицираните закани од злонамерен софтвер. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ПРИНЦИП П6.01 | |
|---|---|
| Формулирајте јасни упатства | • Дефинирајте кои прелистувачи и клиенти за е-пошта се сметаат за целосно поддржани врз основа на стандардите за компатибилност и безбедност.<br>• Наведете критериуми за одредување на поддржан софтвер, земајќи ги предвид факторите како што се поддршката од провајдерот и опоравување од дадена ранливоста. |
| Спецификација на опсегот | • Јасно наведете ја применливоста на политиката за сите вработени, изведувачи и продавачи на трети лица кои пристапуваат до системите на организацијата. |

| | |
|---|---|
| | • Погрижете се политиката да ги покрива и уредите во сопственост на компанијата и личните уреди што се користат за работни цели. |
| Последици од неусогласеност | • Јасно комуницирајте ги последиците од неусогласеноста со политиката, како што е ограничен пристап до ресурсите на организацијата или дисциплинска постапка.<br>• Осигурете се дека последиците се спроведуваат доследно на сите нивоа на организацијата. |
| Редовни процедури за преглед | • Воспоставете процедури за редовно прегледување и ажурирање на списокот со поддржани прелистувачи и клиенти за е-пошта.<br>• Дефинирајте ги улогите и одговорностите за спроведување прегледи, вклучително и ИТ персонал одговорен за следење на ажурирањата за поддршка на продавачот и безбедносните совети. |
| ***ПРИНЦИП П6.02*** | |
| Комуникација за барања | • Јасно пренесете ги барањата за користење на најновите верзии на поддржани прелистувачи и клиенти за е-пошта до сите засегнати страни.<br>• Обезбедете тековни потсетници и ажурирања за да се обезбеди свесност и усогласеност. |
| Упатство за ажурирања | • Обезбедете детални упатства за тоа како корисниците можат да проверуваат и инсталираат ажурирања, вклучувајќи инструкции за конфигурирање на автоматско ажурирање онаму каде што е достапно.<br>• Понудете сесии за обука или ресурси за да им помогнете на корисниците ефективно да го ажурираат нивниот софтвер. |
| Следење на усогласеноста | • Спроведување механизми за следење на усогласеноста, како што се автоматско скенирање за застарени верзии на софтвер или редовни ревизии на инсталираните апликации.<br>• Воспоставување на прагови за прифатливи нивоа на усогласеност и дефинирање на процедури за ескалација за решавање на прашањата за неусогласеност. |
| Исклучоци за ракување | • Воспоставете процедури за справување со исклучоци, како што се наследените апликации кои бараат специфични верзии на прелистувач или клиент за е-пошта.<br>• Дефинирајте ги критериумите за доделување исклучоци и осигурете се дека ризиците поврзани со наследените апликации се соодветно ублажени преку алтернативни контроли. |
| ***ПРИНЦИП П6.03*** | |
| Евалуација на решенија за филтрирање | • Спроведете темелна евалуација на решенијата за филтрирање DNS, земајќи ги предвид факторите како што се доводите за разузнавање за закани, приспособливите политики за филтрирање и леснотијата на интеграција.<br>• Вклучете ги засегнатите страни од тимовите за ИТ, безбедност и операции во процесот на евалуација за да се обезбеди усогласување со организациските потреби. |

| | |
|---|---|
| Интеграција и конфигурација | • Интегрирајте го филтрирањето DNS во мрежната инфраструктура на организацијата и конфигурирајте ги политиките за филтрирање за да го блокирате пристапот до категориите на веб-локации за кои е познато дека имаат злонамерен софтвер, содржина за фишинг или друга злонамерна активност.<br>• Тестирајте ги конфигурациите во контролирана средина пред целосно распоредување за да се обезбеди компатибилност и ефективност. |
| Мониторинг и истрага | • Спроведете процеси за следење на DNS сообраќајот за пронаоѓање на знаци на сомнителни или неовластени обиди за пристап.<br>• Воспоставете процедури за истражување на аномалии и одговор на потенцијални безбедносни инциденти идентификувани преку предупредувања за DNS филтрирање. |
| ***ПРИНЦИП П6.04*** | |
| Изработка на образовни материјали | • Развијте едукативни материјали, како што се модули за обука, презентации или информативни видеа, кои ја објаснуваат целта и придобивките од DNS филтрирањето на едноставен јазик.<br>• Приспособете ги едукативните материјали за различни групи корисници, обезбедувајќи релевантни примери и сценарија кои резонираат со нивните улоги и одговорности. |
| ***ПРИНЦИП П6.05*** | |
| Сеопфатен каталог | • Користете автоматски алатки или скрипти за да извршите сеопфатен попис на сите приклучоци за прелистувачи и клиенти за е-пошта, екстензии и додатоци инсталирани низ средствата на организацијата.<br>• Документирајте суштински детали за секој додаток, вклучувајќи име, верзија, продавач, датум на инсталација и нивоа на дозволи/пристап. |
| Анализа на потребата | • Развијте критериуми или упатства за анализа на потребата и статусот на авторизација на приклучоците и додатоците, земајќи ги предвид факторите како што се деловната функција, влијанието врз безбедноста и барањата за усогласеност.<br>• Прегледајте го секој додаток според утврдените критериуми за да одредите дали е усогласен со потребите на организацијата и придонесува за продуктивноста без да се загрози безбедноста. |
| Процедури за овластување | • Добијте соодветни одобренија или овластувања од релевантни засегнати страни, како што се ИТ администратори, раководители на оддели или службеници за безбедност, за инсталирање или задржување овластени приклучоци и додатоци.<br>• Документирајте го образложението зад одлуките за овластување или одбивање на одредени приклучоци и додатоци, обезбедувајќи транспарентност и одговорност во процесот на овластување. |

| ***ПРИНЦИП П6.06*** | |
|---|---|
| Процедури за идентификација и отстранување | • Развијте процедури или работни текови за систематско идентификување на неовластени или непотребни додатоци и додатоци врз основа на резултатите од процесот на попис и анализа.<br>• Потребно е спроведување на автоматизирани или рачни методи за отстранување на неовластени приклучоци и додатоци од крајни уреди, клиенти за е-пошта и веб-прелистувачи |
| Комуникација со корисниците | • Комуницирајте со засегнатите корисници за да ги објасните причините за отстранување на приклучокот и да дадете насоки за алтернативни решенија или одобрени алтернативи.<br>• Понудете ресурси за обука или поддршка за да им помогнете на корисниците непречено да преминат кон одобрени приклучоци и додатоци. |
| ***ПРИНЦИП П6.07*** | |
| Идентификација на закани: | • Идентификувајте ги вообичаените типови на датотеки поврзани со злонамерен софтвер, напад со софтвер за уцена (ransomware) или други безбедносни закани што може да се пренесат преку додатоците на е-пошта.<br>• Користете разузнавачки информации за закани и безбедносни совети за да останете ажурирани за новите закани и вектори за напади кои се базирани на датотеки. |
| Конфигурација на правилата на главен порт | • Конфигурирајте ги правилата за главен порт за е-пошта за автоматско отфрлање или карантин на влезните е-пораки што содржат прилози на датотеки што се совпаѓаат со наведените екстензии на датотеки поврзани со познати закани.<br>• Редовно прегледувајте ја и ажурирајте ја листата на блокирани екстензии на датотеки врз основа на новите закани, трендовите во индустријата и изворите за безбедносно разузнавање. |

## 7. ОДБРАНА ОД ЗЛОНАМЕРЕН СОФТВЕР (И АНАЛИЗА)

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| 1 | **7.1** Изберете реномирано решение за одбрана од злонамерен софтвер погодни за потребите на организацијата, земајќи ги предвид факторите како што се компатибилноста, ефективноста и леснотијата на управување.<br>**7.2** Воведете го избраниот софтвер за одбрана од злонамерен софтвер на сите средства од организацијата за да обезбедите сеопфатна покриеност на различни уреди.<br>**7.3** Овозможете автоматско ажурирање на софтверот за заштита од злонамерен софтвер за да може да ги следите најновите дефиниции за закани и безбедносни закрпи, обезбедувајќи оптимална заштита од новите закани.<br>***7.4*** Воспоставете политика која наложува автоматско ажурирање на софтверите за одбрана од злонамерен софтвер на сите средства на организацијата, обезбедувајќи конзистентност и придржување до најдобрите безбедносни практики. |
| 2 | **7.5** Редовно проверувајте дали автоматските ажурирања се овозможени и функционираат правилно на сите средства за да се одржи ефективноста на софтверот за одбрана од злонамерен софтвер.<br>**7.6** Конфигурирајте редовни и закажани скенирања на злонамерен софтвер на сите средства за проактивно откривање и отстранување на сите софтвери или потенцијални закани, подобрувајќи ја целокупната безбедносна слика.<br>**7.7** Развијте и имплементирајте процес на управување со промени (Change Management). |
| 3 | **7.8** Имплементирајте централизирано управување на софтверот за одбрана од злонамерен софтвер за да се насочи распоредувањето, конфигурацијата и следењето низ сите средства на организацијата, обезбедувајќи конзистентност и ефикасност во управувањето со безбедносните мерки.<br>**7.9** Овозможете заштита во реално време кај софтверот за одбрана од злонамерен софтвер за активно следење и блокирање на злонамерните активности во реално време, обезбедувајќи заштита во реално време од нови закани.<br>**7.10** Прилагодете ги ажурирања во време на неактивни часови за да го минимизирате нарушувањето на крајните корисници, истовремено обезбедувајќи навремена заштита од новите закани, одржувајќи ја безбедноста без нарушување на продуктивноста.<br>**7.11** Интегрирајте го софтверот за одбрана од злонамерен софтвер со системите за безбедносни информации и управување со настани (SIEM) или платформите за безбедносна оркестрација, автоматизација и одговор (SOAR) за да ги зголемите способностите за откривање и одговор на закани, овозможувајќи ефикасно справување со безбедносни инциденти.<br>**7.12** Имплементирајте напредни техники за откривање на злонамерен софтвер, како што се анализа на однесувањето и изолирана околина (sandboxing), за да ги идентификувате и ублажите нулти ден заканите и софистицираните варијанти на злонамерен софтвер, подобрувајќи ја способноста за откривање и одговор на новите. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***ПРИНЦИП П7.01*** | |
|---|---|
| Репутација и соодветност | • Изберете реномирано решение против злонамерен софтвер приспособено на барањата на организацијата, земајќи ги предвид факторите како што се компатибилноста, ефективноста против познати закани и леснотијата на управување.<br>• Дадете приоритет на решенија со докажано искуство во справувањето со заканите од злонамерен софтвер релевантни за индустријата и опкружувањето на организацијата. |
| Приспособливост и флексибилност | • Изберете решение способно да се зголемува со растот на организацијата и приспособливо на развојните безбедносни потреби, вклучувајќи поддршка за различни крајни точки и мрежни средини.<br>• Оценете решенија кои нудат флексибилност во опциите за имплементација, како што се облак-базирани, на лице место (on-premises), или хибридни модели, за да се усогласат со инфраструктурните преференции на организацијата. |
| ***ПРИНЦИП П7.02*** | |
| Универзална покриеност | • Обезбедете сеопфатна покриеност со распоредување на избраниот софтвер за заштита од малициозни закани низ сите средства на организацијата, вклучувајќи ги и десктоп компјутерите, лаптопите, серверите, мобилните уреди и сите други релевантни крајни точки.<br>• Спроведување на процедури за распоредување кои опфаќаат различни оперативни системи и типови на уреди за да се одржи конзистентноста и ефективноста низ системот на организацијата. |
| Темелна имплементација | • Придржувајте се до стандардизираните практики за распоредување за да се обезбеди униформност и комплетност во процесот на инсталација, минимизирајќи го ризикот од празнини или превиди во покриеноста со заштитата.<br>• Потврдете го успешното распоредување на секое средство и спроведете проверки за валидација за да потврдите правилно функционирање и интеграција со постојната безбедносна инфраструктура. |
| ***ПРИНЦИП П7.03*** | |
| Автоматски ажурирања | • Овозможете автоматско ажурирање за софтверот против злонамерен софтвер за да обезбедите навремена испорака на најновите дефиниции за закани, безбедносни закрпи и подобрувања на софтверот.<br>• Спроведувајте механизми за автоматизирање на процесот на ажурирање на сите средства на организацијата, намалувајќи ја зависноста од рачна интервенција и минимизирајќи ги пропустите поврзани со ажурирањето. |

| | |
|---|---|
| Спроведување на политика | • Воспоставете и спроведувајте политики кои наложуваат автоматско ажурирање на датотеките со потпис против злонамерен софтвер на сите средства на организацијата, обезбедувајќи доследно придржување до најдобрите безбедносни практики.<br>• Редовно прегледувајте и ажурирајте ги политиките за ажурирање за да се приспособат на промените на заканите, технолошкиот напредок и организациските барања. |
| ***ПРИНЦИП П7.04*** | |
| Развој на полиси | • Развијте и документирајте политики кои задолжително го исклучуваат автоматското стартување и автоматското пуштање (autorun и autoplay) на сите преносливи медиуми на средствата на организацијата, со цел да се намали ризикот од ширење на злонамерен софтвер.<br>• Јасно доставете ги упатствата за политиките до крајните корисници преку сесии за обука, кампањи за подигање на свеста и пишани материјали за промовирање на разбирањето и усогласеноста. |

## 8. УПРАВУВАЊЕ СО МРЕЖНА ИНФРАСТРУКТУРА

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **8.1** Регулирајте го физичкиот пристап до опрема за откривање на потенцијални закани за сајбер безбедноста.<br>**8.2** Специјалните администраторски работни станици се чуваат одделени од главната мрежа, без пристап до интернет.<br>**8.3** Само овластен и сертифициран персонал треба да врши поправки и сервис на опремата.<br>***8.4*** Одржувајте ажуриран каталог на мрежните уреди, вклучувајќи хардверски и софтверски конфигурации, верзии на фирмвер и дијаграми за мрежна топологија. |
| **2** | **8.5** Одржувајте и ажурирајте ги дијаграмите на архитектурата и документацијата на мрежниот систем, особено по значителни промени.<br>**8.6** Спроведување на контроли за сегментација на мрежата, како што се заштитни ѕидови, VLAN (виртуелни локални мрежи) и листи за контрола на пристап (ACL), за да се изолира и раздели мрежниот сообраќај помеѓу различни зони.<br>**8.7** Сегментирајте ја мрежата во различни зони или сегменти врз основа на нивоата на доверба, деловните функции и безбедносните барања.<br>**8.8** Употреба на стратегии како сегментација, ограничување на пристапот и обезбедување дека мрежата секогаш е во функција.<br>**8.9** Применете го принципот на минимална привилегија за ограничување на комуникацијата помеѓу мрежните сегменти, минимизирајќи го влијанието на безбедносните инциденти и можноста за латерално движење на напаѓачите.<br>***8.10*** Деталите за внатрешната мрежа и системската конфигурација, услугите на директориумот поврзани со вработени или уреди и друга чувствителна технологија не се јавно достапни. |
| **3** | ***8.11*** Спроведете контроли за управување со промени со кои ќе се овозможи преглед, одобрување и следење на промените на мрежните конфигурации, осигурувајќи дека се имплементирани само овластени и документирани промени. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П8.01*** | |
|---|---|
| Погрижете се да се воспостават физички безбедносни мерки за откривање и одговор на потенцијалните закани за сајбер-безбедноста | • Опремете ги критичните области со камери за следење и снимање активности околу чувствителна или критична инфраструктура.<br>• Користете читачи на картички, биометриски скенери и безбедносни картички за да го контролирате пристапот до чувствителните локации, осигурувајќи дека може да пристапи само овластен персонал.<br>• Спроведување строги политики и процедури за управување со посетителите, вклучително и придружба во безбедносни области и евидентирање на сите влезови и излези.<br>• Спроведување на редовни физички безбедносни проверки за да се идентификуваат и поправат потенцијалните пропусти како што се необезбедени влезни точки или застарени системи со камери. |

| | |
|---|---|
| | • Осигурете се дека записите за физичка безбедност (на пр., записи за пристап, видео снимки) се прегледуваат заедно со системите за сајбер-безбедност за откривање поврзани настани.<br>• Редовно обучувајте го безбедносниот персонал за препознавање на безбедносни закани и спроведување вежби за одговор при итни случаи за да се подобри подготвеноста за нарушување на физичката безбедност.<br>• Вклучете протоколи за нарушување на физичката безбедност во поширокиот план за одговор на инциденти во сајбер-безбедноста, обезбедувајќи координиран одговор на инцидентите што ги опфаќаат двата домени. |
| ***Принцип П8.02*** | |
| Одделете ги административните / контролните системи | • Каде што е можно, назначете компјутери и/или системи за контрола за административни задачи кои имаат соодветни граници со главната мрежа за да се спречи вкрстена контаминација.<br>• Погрижете се овие администраторски компјутери да немаат пристап до Интернет за да се намали ризикот од надворешни закани или, доколку тоа не е можно, ограничете ја таквата врска колку што е разумно можно.<br>• Применете ги највисоките безбедносни поставки, вклучително и користење на заштитни ѕидови и ограничени кориснички дозволи.<br>• Спроведувајте годишни ревизии за да се обезбеди усогласеност со политиките за изолација и да се потврди дека не се воспоставени неовластени врски. |
| ***Принцип П8.03*** | |
| Примена и имплементација на заштитни мерки за мрежите за управување. | • Определените мрежи се користат за уреди за управување, т.е. имплементираат посебен VLAN за управување или физички посебна инфраструктура,<br>• Безбедносни канали, на пр., со користење на VPN, SSH, итн.<br>• Мрежите се дизајнирани и конфигурирани да ги ограничат можностите за неовластен пристап до информациите што транзитираат низ мрежната инфраструктура. Организациите треба да користат што повеќе од следниве технологии за да го исполнат ова барање:<br>○ безбедност на портите на свичевите за да се ограничи пристапот и да се оневозможат сите неискористени порти.<br>○ рутери и заштитни ѕидови сегрегираат делови од мрежата врз основа на потреба да се знае.<br>○ IPSEC/IP верзија 6<br>○ шифрирање на ниво на апликација<br>○ автентикација на мрежни рабови.<br>○ Ограничете и управувајте со уредите на крајните корисници кои комуницираат со мрежата на организацијата преку различни техники за филтрирање |

| | |
|---|---|
| | ○ IPS/IDS за откривање/спречување на малициозни активности во мрежата.<br>• Погрижете се мрежната инфраструктура да биде ажурирана. Примерите за имплементации вклучуваат извршување на најновото стабилно издание на софтвер. Прегледувајте ги верзиите на софтверот месечно, или почесто, за да ја потврдите поддршката на софтверот.<br>• Воспоставете и одржувајте безбедна мрежна архитектура која мора да се однесува на сегментацијата, најмалку привилегии и достапност.<br>• Прегледувајте ја и ажурирајте ја документацијата годишно или кога ќе се случат значајни промени на организацијата што може да влијаат на оваа заштита.<br>• Осигурете се дека записите на мрежата се соодветно изолирани и поддржани во согласност со вашите планови за обновување после катастрофа и континуитет на бизнисот.<br>• Воспоставете и одржувајте посветени компјутерски ресурси, физички или логички одвоени, за сите административни задачи или задачи кои бараат административен пристап. Компјутерските ресурси треба да бидат сегментирани од примарната мрежа на организацијата и да не им се дозволува пристап до интернет.<br>• Пресликувањето на транкот/портата НЕ СМЕЕ да се користи на свичеви кои управуваат со VLAN со различни класификации (на пр. овде внесете национални типови класификација) |
| ***Принцип П8.04*** | |
| Донесување и спроведување на заштитни мерки на мрежите за управување | • Обезбедете безбедна сегментација на мрежата и механизми за контрола на пристап за заштита на чувствителните средства и минимизирање на влијанието на безбедносните инциденти.<br>• Поделете ја мрежата на различни зони или сегменти врз основа на нивоата на доверба, функции и безбедносните барања.<br>• Класифицирајте ги средствата и ресурсите врз основа на нивната чувствителност и барањата за пристап.<br>• Применете го принципот на минимална привилегија за ограничување на комуникацијата помеѓу мрежните сегменти, осигурувајќи дека се дозволени само неопходните врски.<br>• Користете правила за заштитен sид, VLAN и списоци за контрола на пристап (ACL) за да наметнете ограничувања за комуникација и да го ограничите страничното движење на потенцијалните напаѓачи.<br>• Спроведете контроли за управување со промени за прегледување, одобрување и следење на промените во мрежните конфигурации.<br>• Одржувајте ажуриран попис на мрежните уреди и конфигурации за да ги олесните процесите за управување со промени. |

| | |
|---|---|
| | • Осигурете се дека деталите за внатрешната мрежа и системските конфигурации, како и услугите за директориуми поврзани со вработени или уреди, не се јавно достапни за неовластен персонал.<br>• Спроведувајте мерки како што се зацврстување на мрежата, шифрирање и контроли за пристап за заштита на чувствителните информации од неовластен пристап или откривање. |

## 9. МОНИТОРИРАЊЕ И ОДБРАНА НА МРЕЖАТА

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | ***9.1*** Редовно прегледување и анализа на записите, шаблоните на мрежниот сообраќај и системската активност за да се идентификуваат индикаторите за компромитирање (IOC) и потенцијалните безбедносни нарушувања.<br>***9.2*** Имплементирајте хост базирани решенија за спречување на нарушувања. |
| **2** | **9.3** Спречете неовластен и ненамерен пренос на информации преку споделени системски ресурси.<br>**9.4** Осигурете се дека далечинските уреди користат VPN и се поврзуваат со основната инфраструктура.<br>***9.5*** Воведете подмрежи за јавно достапни системски компоненти кои се физички или логички одвоени од внатрешната мрежа. |
| **3** | **9.6** Имплементирајте напредни SIEM системи и одговор на инциденти.<br>**9.7** Воспоставете и управувајте со криптографски клучеви за криптографија што се користат во организациски ИКТ системи.<br>**9.8** Филтрирајте го сообраќај меѓу различни делови од мрежата.<br>**9.9** Распоредете решенија за спречување на нарушувања во мрежата и контрола на пристап на ниво на порт за специфични технологии или протоколи.<br>**9.10** Спречете далечински уреди истовремено да воспоставуваат не-далечински врски со организациските системи и да комуницираат преку некоја друга врска со ресурси во надворешни мрежи (т.е., split tunnelling).<br>**9.11** Прекинете ги мрежни врски поврзани со комуникациски сесии на крајот од сесиите или по дефиниран период на неактивност.<br>**9.12** Забранете далечинско активирање на уреди за колаборативно работење (мрежни бели табли, камери и микрофони) и обезбедете информации на корисниците кога уредот е вклучен. Заштита на автентичноста на комуникациските сесии.<br>**9.13** Заштитете веб апликација(и) од сајбер закани што се својствени за веб технологиите. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П9.01*** | |
|---|---|
| Постојано следете и анализирајте безбедносни записи, мрежниот сообраќај и системските активности за да откриете индикатори за компромитирање (IOC) и да спречите безбедносни прекршувања. | • Воспоставете рутина (на пр., континуирано, часовно, дневно, неделно, месечно) за прегледување на безбедносните записи, мрежниот сообраќај и системската активност. Прилагодете ја фреквенцијата врз основа на чувствителноста на информациите и критичноста на системот.<br>• Создадете упатства и списоци за проверка за идентификување на абнормални активности и потенцијални индикатори за компромитирање (IOC) како што се невообичаен излезен сообраќај, скокови во пристапот до податоци или обиди за неовластен пристап.<br>• Документирајте јасни мапи на процеси за тријажа и ескалација, вклучувајќи упатства за постапување кога ќе бидат идентификувани несоодветни настани.<br>• Периодично симулирајте безбедносни инциденти за да ја тестирате ефективноста на вашите протоколи за следење и анализа и да ги прилагодите врз основа на најдените резултати. |
| ***Принцип П9.02*** | |
| Надгледувајте и управувајте со мрежите | • Треба да се воведат соодветни решенија (на пр. заштитен ѕид, VLAN тип), кои овозможуваат филтрирање и разделување на сообраќајот кон ИКТ системите одговорни за поддршка на критичните процеси спроведени од операторот.<br>• Директниот пристап до Интернет од ИКТ системите одговорни за поддршка на критичните процеси спроведени од операторот треба да биде спречен, а доколку е дозволен, причините и пристапот треба да бидат документирани како дел од внатрешните политики.<br>• Веб-содржините треба да бидат филтрирани – пристапот до малициозни домени и интернет адреси, реклами и анонимни мрежи треба да се регистрира, следи и блокира. Доколку е одобрено, треба да се создадат и редовно да се прегледуваат соодветни „листи на дозвола“.<br>• По правило, секој непотребен и неовластен мрежен сообраќај (дојдовен или излезен) мора да биде блокиран (на пр. со користење IPS/IDS решенија и апликациски заштитени ѕидови), вклучително и оној генериран од недоверливи апликации.<br>• Користете само доверливи DNS сервери, а детално филтрирање на DNS барањата треба да се спроведе.<br>• Мрежниот сообраќај кон и од компјутерите каде што се чуваат критични податоци или оние што се одговорни за поддршка на критичните процеси што ги извршува операторот, како и сообраќајот што го минува периметарот на мрежата на организацијата, треба да се запишува и да биде достапен за ревизија за откривање и анализа на инциденти.<br>• Функциите за „безбедност на порти“ (port security) треба да се користат на мрежните прекинувачи.<br>• Исклучете ги неупотребуваните услуги што не се потребни за работа на одредена работна станица, како што се RDP, |

| | |
|---|---|
| | AutoRun, LanMan, SMB/NetBIOS, LLMNR, WPAD и протоколи, на пр. DHCP, IPv6, IPX, итн. |
| ***Принцип П9.03*** | |
| Одделете ги мрежите на информативните услуги, корисниците и информациските системи | • Поделбата на мрежата во одделени мрежни домени е еден метод за надгледување на безбедноста на големи мрежи. Разделувањето може да се направи физички или логички. Независно од методот на распределба, границите на секој домен и барањата за пристап до секој домен мора јасно да бидат дефинирани.<br>• Пристапот меѓу домени е можен, но се препорачува да се контролира со уреди како што се firewall или филтрирачки рутер. Обидите за поврзување што не се однапред дефинирани треба да се следат и анализираат.<br>• Ограничете ги уредите со ниско ниво на доверба (на пр. IoT и BYOD уреди) и ограничете го мрежниот пристап до дискови и складишта на податоци врз основа на функцијата, а доколку се дозволени, причините и пристапот треба да бидат документирани како дел од внатрешните политики.<br>• Мрежни прекинувачи од слој 3 (OSI модел) се користат за разделување на LAN во VLAN-ови. Прекинувач од слој 3 може да извршува рутирање помеѓу VLAN-ови со брзина на кабелска врска и предвидлива перформанса, но можеби нема да обезбеди исто ниво на безбедност и контрола на политики како што го прави огнени ѕидови од идна генерација (NGFW). |
| ***Принцип П9.04*** | |
| Спроведување на мрежа на демилитаризирана зона (DMZ) за зголемена организациска безбедност | • Организацијата треба да создаде DMZ (демилитаризирана зона) како периметарска мрежа која штити и додава дополнителен слој на безбедност на внатрешната локална мрежа на организацијата од недоверлив сообраќај.<br>• Мрежата со демилитаризирана зона (DMZ) ѝ овозможува на организацијата пристап до недоверливи мрежи, како што е интернетот, додека осигурува дека нејзината приватна мрежа или LAN останува безбедна.<br>• Каде што е можно, организациите треба да го складираат следново во DMZ:<br>○ надворешно ориентирани услуги и ресурси.<br>○ сервери за системот за имиња на домени (DNS),<br>○ Протокол за пренос на датотеки (FTP),<br>○ е-пошта,<br>○ прокси,<br>○ и веб сервери.<br>• Овие сервери и ресурси треба да бидат изолирани и со ограничен пристап до LAN, за да се осигури дека можат да се пристапат преку интернет, но внатрешниот LAN да остане недостапен. |
| ***Принцип П9.05*** | |
| Спроведете сеопфатен и слоевит безбедносен пристап за заштита на | • Користете HTTPS протокол наместо HTTP за безбедна комуникација. HTTPS ги шифрира податоците во транзит помеѓу клиентот и серверот, спречувајќи прислушување и мешање на податоците.<br>• Спроведете безбеден механизам за автентикација и авторизација за да се осигура дека само овластени корисници |

| | |
|---|---|
| програмабилните апликациски интерфејси (API) | можат да пристапат до API. Размислете за користење токени, протокол OAuth2 или клучеви API.<br>• Потврдете ги сите внесувања на корисникот за да спречите каква било злонамерна активност преку пристап до API.<br>• Потврдете ги сите влезни податоци за да спречите напади со инјектирање, како што се нападите со инјектирање SQL или напади со скриптирање мегу сајтовите (XSS).<br>• Спроведувајте ограничување на стапката за да се спречат DoS напади со ограничување на бројот на барања што корисникот може да ги направи во даден временски период. Ова може да се направи со конфигурирање на мрежните уреди.<br>• Водете евиденција за сите барања и одговори на API и следете ги за каква било сомнителна активност.<br>• Користете ги најновите безбедносни стандарди: проверете дали API ги користи најновите безбедносни стандарди и протоколи, како што е TLS 1.2 или повисоко, и избегнувајте да користите застарени или слаби криптографски алгоритми.<br>• Спроведете редовни безбедносни тестови и ревизии за да се идентификуваат сите пропусти или слабости во API и навремено да се решат. |
| ***Принцип П9.06*** | |
| Применете ја длабинската одбрана за WebApps | • Развијте веб-апликации, имајќи ги предвид најдобрите безбедносни практики.<br>○ Безбедносни платформи за извршување:<br>○ Распоредете апликации на доверливи апликациски сервери (на пр. Apache, Glassfish, WebSphere и WebLogic)<br>○ Осигурајте се дека платформите се постојано ажурирани.<br>• Редовни безбедносни проценки:<br>○ Спроведете тестирање за пенетрација за да откриете нови пропусти.<br>○ Вклучете безбедносни прегледи како дел од животниот циклус на развој.<br>○ Следете ги соодветните и воспоставени упатства (на пр. OWASP топ 10)<br>• Спроведете WAF за да се обезбеди дополнителен безбедносен слој. |

## 10. ОБУКА ЗА БЕЗБЕДНОСНА СВЕСТ И ВЕШТИНИ

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **10.1.** Воспоставете и одржувајте програма за подигање на свеста за сајбер безбедноста.<br>**10.2.** Осигурете се дека персоналот е свесен за важечките безбедносни стандарди, политики и процедури и поврзаните безбедносни ризици поврзани со нивните активности во системот.<br>***10.3.*** Осигурете се дека персоналот е редовно обучен за извршување на нивните должности и одговорности за сајбер-безбедност специфични за улогата во согласност со релевантното законодавство, политики и процедури. |
| **2** | ***10.4.*** Обезбедете обука за подигање на свесноста за препознавање и известување на потенцијални индикатори за внатрешна закана. |
| **3** | ***10.5.*** Спроведете кампања за промовирање и подигање на свесноста за сајбер безбедност меѓу релевантните добавувачи, клиенти и трети засегнати страни. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П10.01*** | |
|---|---|
| Целокупна програма за подигање на свеста за сајбер безбедноста | • Програма за подигање на свеста за сајбер безбедноста треба да биде прилагодена и дефинирана заедно со соодветни буџети наменети за нејзино спроведување.<br>• Развијте и документирајте програма за свесност и обука која се однесува на целта, опсегот, улогите, одговорностите, посветеноста на управувањето, координацијата меѓу организациските субјекти и усогласеноста.<br>• Развијте и документирајте процедура за олеснување на спроведувањето на програмата за подигање на свеста и обука.<br>• Вклучете неколку активности за подигање на свеста преку соодветни физички или виртуелни канали како што се кампањи, брошури, постери, билтени, веб-страници, информативни сесии, брифинзи, модули за е-учење, интранет и е-пошта.<br>• Прегледајте ја и ажурирајте ја програмата за подигање на свеста и обука еднаш годишно.<br>• Раководството на организацијата треба да има програма за подигање на свеста за сајбер-безбедноста, проширена според позицијата што ја има (на пр., надзор над вработените, специфичните улоги и одговорности, итн.). |

| ***Принцип П10.02*** | |
|---|---|
| Целокупна програма за обука за сајбер безбедност | • Целиот персонал на владината организација и, онаму каде што е релевантно, изведувачите, клиентите и трети лица или засегнати страни, треба да добијат соодветна обука за свесноста за безбедноста во однос на политиките и процедурите на организацијата, релевантни за нивната работна функција, улоги, одговорности и вештини.<br>• Потребна е изработка на годишен план за спроведување на обуките за сајбер безбедност.<br>• Планирајте и спроведете почетна програма за обука на свеста за секој нов вработен или во секој случај на трансфер на вработениот од друга организација.<br>• Идентификувајте соодветни обуки за технички тимови чии улоги бараат специфични групи на вештини и експертиза.<br>• Високите раководители и раководството на организацијата треба да бидат обучени конкретно во согласност со нивните улоги и одговорности.<br>• Програмата за обука треба да разгледа различни форми/формати, како што се:<br>  ○ предавања или само студии, менторирани од стручен персонал или консултанти,<br>  ○ ротирачки членови на персоналот за следење различни активности,<br>  ○ регрутирање веќе квалификувани луѓе,<br>  ○ ангажирање консултанти.<br>• Обуките треба да бидат дизајнирани да вклучуваат интерактивни елементи, особено како што се:<br>  ○ Презентација на вистински примери на напади.<br>  ○ Развивање игри или натпревари со безбедносна тема кои го предизвикуваат персоналот да го примени своето знаење во различни сценарија.<br>  ○ Инкорпорирање симулации или вежби кои имитираат ситуации од реалниот живот што му овозможуваат на персоналот да ги практикува своите вештини во контролирана средина.<br>  ○ Нудење стимулации или награди за успешно завршување на модулите за обука или постигнување високи оценки за оценување.<br>  ○ Привилегираните корисници ги разбираат нивните улоги и одговорности<br>• Обезбедете релевантни обуки за засегнатите страни од трети страни (на пример, добавувачи, клиенти, партнери) за да ги разберат нивните улоги и одговорности пред да бидат ангажирани.<br>• Обучете ги вработените да ги препознаваат обидите за социјално инженерство врз нив и да не откриваат какви било информации што би можеле да ги нарушат безбедносните политики на организацијата, како што се за време на социјални собири, јавни настани и настани за обука. |

| ***Принцип П10.03*** | |
|---|---|
| Механизми и KPI за следење и евалуација | • Воспоставете механизми и клучни индикатори за успешност за следење и евалуација на ефективноста и ефикасноста на програмите за подигање на свеста и обука.<br>• Редовно прегледувајте и ажурирајте ја содржината на обуката за безбедност и свесноста за да ги одрази соодветно новите ризици, современите закани, потенцијалните предизвици и промените во инфраструктурата за информатичка технологија на организацијата или применливите закони и регулативи.<br>• Секоја обука треба да биде проследена со анализа, за да се утврди ефективноста на програмата, вклучително и одржување на евиденција за присуство на програми за подигање на свеста за безбедноста. |

# 11. УПРАВУВАЊЕ НА ДАВАТЕЛИ НА УСЛУГИ (И ДОБАВУВАЧИ/ТРЕТА СТРАНА).

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **11.1.** Развијте, документирајте и споделете политика за управување со ризик во синџирот на снабдување, опфаќајќи минимални безбедносни барања за договори со трети страни.<br>**11.2.** Утврдете и договорете безбедносни барања за информации, во соработка со надлежниот орган (каде што е применливо), со секој добавувач/провајдер на услуги врз основа на видот на односот со добавувачот/провајдерот на услуги.<br>**11.3.** Дефинирајте и спроведете процеси и процедури заедно со надлежниот орган, каде што е применливо, за да се управуваат безбедносните ризици поврзани со ИКТ производите и услугите во синџирот на снабдување.<br>**11.4.** Редовно следете, прегледувајте и прегледајте ги сите услуги обезбедени од трети страни. |
| **2** | **11.5.** Во соработка со надлежниот орган каде што е применливо, редовно следете, прегледувајте и оценувајте ги промените во практиките за безбедност на информации и испораката на услуги на добавувачот.<br>**11.6.** Водете евиденција за безбедносни инциденти поврзани со или предизвикани од трети страни.<br>**11.7.** Прегледувајте и ажурирајте ја политиката за управување со ризик во синџирот на снабдување еднаш годишно, земајќи ги предвид претходните инциденти, промени и слично. |
| **3** | **11.8.** Оценувајте и прегледувајте ги ризиците поврзани со синџирот на снабдување поврзани со добавувачите или услугата што тие ја обезбедуваат. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П11.01*** | |
|---|---|
| Политики и постапки за управување со ризик во синџирот на снабдување | • Развијте, документирајте и споделете политика за управување со ризикот од синџирот на снабдување, која ќе го дефинира следново:<br>○ Цел, опсег, улоги, одговорности, посветеност на управување, координација меѓу организациските субјекти и усогласеност.<br>○ Политиката мора да биде конзистентна со важечките закони, извршни наредби, директиви, регулативи, политики, стандарди и упатства.<br>• Дефинирајте и спроведете процедури за управување со ризиците за безбедноста на информациите поврзани со ИКТ средствата и услугите во управувањето со синџирот на снабдување, во согласност со политиката.<br>• Назначете службеник или член на персоналот да раководи со развојот, документацијата и ширењето на политиката и процедурите за управување со ризик од синџирот на снабдување. |

| ***Принцип П11.02*** | |
|---|---|
| План за управување со ризик од синџирот на снабдување | • Подгответе план за управување со ризиците од синџирот на снабдување поврзани со истражување и развој, дизајнирање, производство, стекнување, испорака, интеграција, операции и одржување и отстранување на системите, компонентите на системот или системските услуги.<br>• Редовно прегледувајте го и ажурирајте го или во случај на потреба, за справување со заканите, организациските промени или промени на средината. |
| ***Принцип П11.03*** | |
| Договори за услуги | • Наведете безбедносни механизми, нивоа на услуги и барања за управување во сите договори за услуги (во соработка со надлежниот орган каде што е применливо). Доколку се користат услуги од трети страни давателот на услугата треба да биде обврзан да имплементира систем за евиденција на настани во мрежите и ИКТ системите и да развие процедури за архивирање на собраните записи (најмалку за период од 12 месеци).<br>• Секој договор со трета страна треба да содржи одредби со кои се бара од страната редовно да известува за безбедносното држење на услугата(ите), вклучувајќи ги и сите инциденти.<br>• Следниве фактори на ризик треба да се земат предвид при подготовката на договорите со давателите на ИКТ услуги и производи:<br>○ Тековната финансиска и економска состојба на потенцијалниот давател на услуги (при избор на давател на услуги).<br>○ Сопственичката структура, доколку е можно, вклучувајќи ја идентификацијата на вистинските корисници (при изборот на давател на услуги).<br>• Секоја врска со нов партнер треба да започне со договор за доверливост, кој предвидува вистински санкции за секое прекршување. Посебно внимание треба да се посвети на односите со добавувачите на ИКТ решенија или производи кои содржат компјутерски софтвер што може да влијае на оперативниот капацитет на ИТ инфраструктурата на институцијата.<br>• Заедно со обичните елементи, договорот треба да ги содржи, барем, следните специфични елементи:<br>○ опис на очекуваниот опсег на соработка на давателот на услугата, вклучително и трети страни кои дејствуваат во негово име, и кои учествуваат во обезбедувањето на услугата со институцијата во случај на поправање на дефекти. Овој опсег треба да вклучува, но не е ограничен на обезбедување на специфична инфраструктура, персонал и достапност на таков персонал.<br>○ правила за отстранување на пријавени грешки, во форма на таканаречен Договор за ниво на услуги (SLA), кои содржат индикатори за процедурите за соработка, навременоста на отстранување на пријавените грешки како и санкции за доцнење во отстранувањето на грешките и нивно неотстранување. |

| | |
|---|---|
| | ○ Договорите за услуги со развивачите/производителите на софтвер треба да вклучуваат дополнителни SLA во врска со отстранувањето на откриените пропусти, чија употреба може да предизвика ризик од нарушување на функционирањето на ИКТ инфраструктурата на институцијата.<br>○ Договорот за набавка или одржување на софтвер треба да содржи одредби во врска со постапката за управување со промените во овој софтвер и начинот на определување на надоместокот на давателот на услугата за тоа.<br>○ Договорот за набавка на софтвер и хардвер треба да содржи одредби за зголемување на безбедноста од ИКТ закани.<br>• Во случај на ИКТ системи кои поддржуваат критични процеси, треба да се постави барање добавувачот да има осигурителна политика за покривање на загубите предизвикани од неправилно извршување на договорот.<br>• Секој склучен договор треба да биде предмет на анализа на ризик во однос на единствен добавувач обично се поврзува со неповолни одредби за интелектуална сопственост во однос на можноста за развој или користење на производи (обично софтвер) во случај на банкрот на добавувачот или прекин на соработката од страна на добавувачот.<br>• Договорот не треба да содржи одредби кои целосно ја исклучуваат одговорноста на добавувачот или ја ограничуваат неговата одговорност на износи што не одговараат на ризикот поврзан со испораката на производ или услуга што не ги исполнува условите на договорот. |

## 12. БЕЗБЕДНОСНО ТЕСТИРАЊЕ И ПРЕГЛЕД НА КОД

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **12.1.** Нема |
| **2** | **12.2.** Користете ажурирани и доверливи софтверски компоненти од трета страна. |
| **3** | **12.3.** Воспоставете и одржувајте безбеден процес за развој на апликации.<br>**12.4.** Воведете структуриран пристап за извршување безбедносно тестирање и проверка на кодот на апликативниот софтвер пред неговото пуштање во употреба..<br>**12.5.** Воведете механизми за идентификување и отстранување на безбедносните слабости или ранливости откриени за време на процесите на тестирање и преглед на кодот.<br>**12.6.** Статичко и динамичко тестирање за безбедност на апликациите. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П12.01*** | |
|---|---|
| Насоки за безбеден развој | • Развијте и ажурирајте јасни насоки за безбедно развивање апликации, кои ќе ги покриваат клучните области како валидација на внесот и шифрирање на податоците. Овие насоки треба да бидат достапни за сите програмери и редовно ажурирани за да се усогласат со променливите закани.<br>• Соработувајте со безбедносни експерти за да ги потврдите и подобрите овие упатства, обезбедувајќи нивна ефикасност. |
| Прегледи на кодови и статичка анализа | • Воспоставете редовни прегледи на кодови каде што програмерите го проверуваат меѓусебниот код за безбедносни недостатоци, поттикнувајќи култура на одговорност и свесност преку учење и соработка од колеги.<br>• Интегрирајте ги автоматизираните алатки за анализа на статички кодови во развојниот процес за автоматско откривање на потенцијални безбедносни проблеми, спроведувајте редовни скенирања и доставување активна повратна информација до програмерите за решавање на пропустите. |
| Обука за безбедност и свесност | • Одржувајте интерактивни обуки за програмерите за безбедносни практики за кодирање, ранливости и безбедносни рамки, зајакнувајќи го учењето со практични примери.<br>• Започнете кампањи за подигање на свеста во тимовите за развој преку е-пошта, постери и билтени, нагласувајќи ја клучната улога на безбедноста во животниот циклус на софтверот и споделувајќи увид за неодамнешните инциденти и најдобри практики. |

| | |
|---|---|
| ***Принцип П12.02*** | |
| Статичко и динамичко тестирање за безбедност на апликации (статичко тестирање за безбедност на апликации (SAST), динамичко тестирање за безбедност на апликации (DAST)) | • Интегрирајте ги SAST алатките во развојната линија за автоматско скенирање на кодот, нудејќи им непосредна повратна информација на програмерите.<br>• Вклучете ги алатките DAST во фазата на тестирање за да се симулираат напади во реална средина и да се идентификуваат ранливостите на однесувањето во реално време дополнувајќи ја статичката анализа за сеопфатна безбедносна анализа. |
| Имплементирајте механизми за да ги идентификувате и поправите безбедносните закани или ранливости откриени за време на процесите на тестирање и преглед на кодот. | • Воспоставете процедури за идентификување и отстранување на безбедносните закани, доделување улоги и рокови.<br>• Интегрирајте ги пронајдените безбедносни резултати во документот за управувањето со промените, документирајте и справите се со пропустите преку контролирани промени на кодот. |
| ***Принцип П12.03*** | |
| Спроведете безбедносно тестирање во текот на животниот циклус на развој на софтвер | • Интегрирајте безбедносно тестирање за континуирана интеграција/континуирано распоредување (CI/CD) за да го автоматизирате процесот на идентификување и адресирање на безбедносните пропусти во текот на животниот циклус на развој на софтвер. Конфигурирајте ги автоматизираните тестови да се извршуваат автоматски секогаш кога ќе се направат промени во кодот, обезбедувајќи им на програмерите непосредни повратни информации за потенцијалните безбедносни проблеми.<br>• Спроведете безбедносно регресивно тестирање за да се осигурите дека безбедносните контроли и механизми остануваат ефективни додека софтверот се развива со текот на времето. Идентификувајте и решете ги сите регресии или непредвидени последици од промените во кодот кои можат да влијаат на безбедноста на апликацијата. |
| ***Принцип П12.04*** | |
| Спроведување на безбедносни практики за кодирање | • Воспоставете и спроведете безбедносни стандарди и упатства за кодирање за да се промовира употребата на безбедносни практики за кодирање во тимовите за развој. Обезбедете им на програмерите обука и ресурси за да им помогнете да ги разберат и да се придржуваат до овие |

| | |
|---|---|
| | стандарди во текот на животниот циклус на развој на софтвер.<br>• Користете безбедносни развојни рамки и библиотеки кои се проверени за безбедносни пропусти и придржувајте се до најдобрите индустриски практики. Охрабрете ги програмерите да ги користат овие рамки за да го намалат ризикот од внесување на безбедносни недостатоци или пропусти во базата на кодови. |

## 13. ОДГОВОР ПРИ ИНЦИДЕНТИ И ПОВРАТ НА ПОДАТОЦИ

| *НИВО* | *БЕЗБЕДНОСНА МЕРКА* |
|---|---|
| **1.** | **13.1.** Дефинирајте процедури за откривање, оценување и одговор на инциденти, со доделени одговорности за управување со откриените инциденти.<br>**13.2.** Воспоставете и имплементирајте оперативна способност за одговор на инциденти со цел подготовка, откривање и брзо реагирање при инциденти во сајбер просторот. |
| **2.** | **13.3.** Реализирајте соодветни активности по инцидентот.<br>**13.4.** Обезбедете откривање на сајбер закани во реално време за критичните системи и нивните компоненти.<br>**13.5.** Обезбедете компјутерска форензика на компромитираните системи, вклучувајќи анализа на меморијата, анализа на мрежниот сообраќај и “обратно инженерство” на злонамерен софтвер.<br>**13.6.** Истражете ги значајните инциденти и напишете финални извештаи за инцидентите, вклучувајќи ги преземените дејства и препораките за избегнување на повторната појава на овој тип инциденти во иднина. |
| **3.** | **13.7.** Спроведете пронаоѓање на закани (threat hunting).<br>**13.8.** Соработувајте со други институции од областа со цел споделување на информации за индикатори на компромитирање, со цел да се подобрат безбедносните контроли и да ги спречите злонамерните активности.<br>**13.9.** Обезбедете статична и динамична анализа на злонамерен софтвер преку специјализирани алатки за анализа на злонамерен софтвер (сопствено хостирани решенија или решенија во облак).<br>**13.10.** Обезбедете анализа на инциденти преку посебни алатки за анализа. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| *ПРИНЦИП П13.01* | |
|---|---|
| Соодветни активности и процеси за одговор на инциденти | • Преземете ги потребните активности вклучувајќи процеси и процедури за одговор.<br>• Подгответе План за одговор на инциденти што ќе се изврши за време или по појавувањето на сајбер инцидентот.<br>• Организирајте правилна комуникација и координирање на активностите за време на одговор на инцидентите со релевантните чинители, внатрешни и надворешни.<br>• Воспоставете и одржувајте минимум праг/ниво за безбедносни инциденти, вклучувајќи, во најмала рака, разлика помеѓу инцидент и настан.<br>• Поставете процеси или системи за откривање инциденти и имплементирајте стандарди каде што е соодветно.<br>• Поставете напредни системи за откривање закани и одговор на инциденти. |

| | |
|---|---|
| | • Истражете ги известувањата и алармите од системите за откривање.<br>• Формирајте тим за одговор на инциденти. |
| ***ПРИНЦИП П13.02*** | |
| Процедури при одговор на инциденти | • Процедурите треба да вклучуваат минимум:<br>○ структура на известување,<br>○ план за одговор на инцидентот, улоги, одговорности и информации за контакт,<br>○ внатрешни и надворешни комуникациски процеси,<br>○ класификација на инциденти,<br>○ времетраење за човечка реакција на пријавениот инцидент, според типот на инцидентот.<br>○ анализирање, задржување и отстранување на процесите.<br>• Процедурите за известување и истражување на безбедносни инциденти поврзани со апликативен софтвер, вклучувајќи анализа на инциденти и стратегии за избегнување, треба да бидат дел од процедурите за одговор на инцидентот.<br>• За да бидат ефективни, процедурите треба да бидат поддржани со соодветни човечки, технолошки, организациски капацитети и способности.<br>• Редовно правете анализа на релевантните процедури земајќи ги предвид минатите инциденти. |
| Анализа на инциденти и извештаи | • Разберете го влијанието на инцидентите и категоризирајте ги во согласност со плановите за одговор.<br>• Комуницирајте и известувајте за тековните или минати инциденти на трети страни, клиенти и/или владини органи, кога е потребно.<br>• Анализирајте ја основната причина за инцидентот.<br>• Спроведете ги научените лекции – преку идентификување области за подобрување на безбедносната состојба.<br>• Одржувајте процес за вработените да известуваат за забележаните безбедносни инциденти, вклучувајќи временска рамка за известување, персонал на кој треба да се пријави, механизам за известување и минимални информации што треба да се вклучат во пријавата.<br>• Спроведете периодични обуки засновани на сценарија преку истражување на истите во согласност со заканите со кои се соочува организацијата. |
| Улоги и одговорности | • Доделете улоги и соодветни одговорности за управување со инциденти на персоналот од: правна служба, безбедност на информации и објекти, односи со јавноста, човечки ресурси, одговорни за инциденти и аналитичари, секаде каде е применливо. |
| Контакт информации и воспоставување комуникација со релевантните структури | • Воспоставете информации за контакт и поврзување со релевантните органи и страни кои треба да бидат информирани за безбедносни инциденти.<br>• Контактите може да вклучуваат внатрешен персонал, трети страни, органи за спроведување на законот, даватели на сајбер осигурување, релевантни владини агенции, |

| | |
|---|---|
| | партнери од Центарот за споделување и анализа на информации (ISAC) или други засегнати страни.<br>• Одредете механизми за комуникација и известување за време на безбедносен инцидент.<br>• Одржувајте канали со оперативните контакти во релевантните органи, тела и служби кои се неопходни.<br>• Воспоставете врска со релевантните органи за спроведување на законот и регулаторните тела со цел олеснување на соработката за време на истрагите за сајбер форензика и да се усогласени со законските и регулаторните барања. |
| Тестирање на способностите за одговор при инциденти | • Вршете тестови за способности за одговор на инциденти најмалку секоја втора година или почесто ако има потреба. |
| ***ПРИНЦИП П513.03*** | |
| Активности при закрепнување | • Спроведете анализа за да се обезбеди ефективен одговор, да се поддржат активностите за закрепнување, да се преземат активности за спречување на проширување, да се намалат ефектите и да се реши инцидентот.<br>• Поттикнување на меѓусебна соработка:<br>○ Поттикнете ја комуникацијата и соработката помеѓу тимот за одговор на инциденти, персоналот на SOC, ИТ и другите релевантни тимови за да се олесни споделувањето информации и експертиза, подобрувајќи ја целокупната безбедносна состојба.<br>○ Континуирана обука и активности за: подигање на свеста за безбедноста и одговор на инциденти кај аналитичарите на SOC и другиот персонал да се во тек со најновите закани, алатки и најдобри практики. |

# 14. ЗАШТИТА НА ПОДАТОЦИ И ПРИВАТНОСТ

## 14.1 Заштита на системски медиуми

| *Ниво* | *Безбедносни мерки* |
|---|---|
| **1** | **14.1.1.** Заштитете ги системските медиуми што содржат хартиени и дигитални информации кои не се од јавен карактер.<br>**14.1.2.** Организирајте пристап до информации кои не се од јавен карактер на системските медиуми само за овластени корисници.<br>**14.1.3.** Уништете ги или соодветно пребриши ги системските медиуми што содржат информации кои не се од јавен карактер според пропишана процедура пред да ги фрлите или пуштите за повторна употреба.<br>**14.1.4.** Обезбедете начин на идентификација на записите и период на нивно чување, во согласност со барањата на законодавството или регулативите.<br>**14.1.5.** Забранете ја употребата на какви било преносливи уреди за складирање што не ги поседува организацијата, со исклучок во одредени наведени случаи и околности.<br>**14.1.6.** Контролирајте ја употребата на отстранлив медиум на компонентите на системот. |
| **2** | **14.1.7.** Обележете го секој медиум кој содржи информации кои не се од јавен карактер со соодветни ознаки и ограничувања за дистрибуција.<br>**14.1.8.** Надгледувајте го пристапот до медиумите што содржат информации кои не се од јавен карактер и доделете одговорност за медиумите за време на транспортот надвор од контролираните области. |
| **3** | **14.1.9** Поставете криптографски механизми за заштита на доверливоста на информации кои не се од јавен карактер зачувани на дигитални медиуми за време на транспортот, освен ако не се поинаку заштитени со алтернативни физички заштитни мерки.<br>**14.1.10.** Заштитете ја доверливоста на резервните медиуми со информации кои не се од јавен карактер на местата за складирање. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П14.1.01*** | |
|---|---|
| Организациони и технички мерки | Развивање, документирање и спроведување на организационо-технички мерки за заштита на сите медиуми кои содржат информации кои не се од јавен карактер.<br>Мерките да бидат соодветни за медиумите што содржат информации што не се од јавен карактер.<br>Редовно разгледување и прилагодување на мерките според законските барања и современите побарувања.<br>Организацијата треба да го ограничи пристапот до информации кои не се од јавен карактер за системските медиуми на овластени |

| | |
|---|---|
| | корисници преку соодветни пропишани правила и процедури, со точно утврдени овластувања за пристап според работното место и одговорностите. |
| ***Принцип П14.1.02*** | |
| Управување и достапност на системските медиуми после завршување на вработувањето | • Строго да се регулира користењето и достапност на медиумите по престанокот на работниот однос.<br>• Секој вработен по престанокот на работниот однос мора да ги врати сите ресурси (системски медиуми кои содржат информации што не се од јавен карактер) кои му биле доделени на вработениот, како што се:<br>○ Враќањето на сите издадени ИКТ уреди.<br>○ Враќањето на ресурсите треба да се случи и во случај на промена на работното место во ситуација кога вработениот престанува да користи даден ресурс како дел од извршувањето на службените должности. |
| ***Принцип П14.1.03*** | |
| Пребришување и уништување на системски медиуми | • Пребришете или уништете ги системските медиуми што содржат информации што не се јавни пред да се отстранат или пуштат за повторна употреба.<br>• Ова треба да се направи со методи на физичко уништување, како што се сечкање, согорување или демагнетизирање.<br>• Целиот процес на пребришување и отстранување на медиумите треба да се документира, вклучувајќи информации за датумот, видот на медиумот и одговорниот персонал.<br>• Оневозможете читање податоците (со препишување, уништување на операторот итн.) на сите носители на податоци кои трајно ја напуштаат организацијата. |
| Идентификација на записи и период на чување | • Да се обезбеди идентификација на записите и нивниот период на чување, имајќи го предвид релевантното законодавство.<br>• Главната легислатива што треба да се смета за најрелевантна и појдовна точка е Законот за заштита на личните податоци на Република Северна Македонија. |
| ***Принцип П14.1.04*** | |
| Процедури за справување со носачи на податоци и ИКТ опрема при повлекување од употреба | • Креирајте и воведете во пракса процедури за справување со носители на податоци и ИКТ опрема повлечена од тековната употреба.<br>• Направете го ова преку:<br>○ Категоризација на носители на податоци (на пр., преносливи и непреносливи);<br>○ Правила на однесување за секоја категорија.<br>○ Процедурите треба да се однесуваат на издавањето, повлекувањето и преносот на медиумите.<br>• Процедурите треба да вклучуваат блокирање на неодобрени CD/DVD/USB медиуми за поврзување со неодобрени телефони, таблети и уреди со Bluetooth/Wi-Fi/3G/4G/5G. Ова барање се однесува на ИКТ системите одговорни за поддршка на критичните процеси што ги спроведува институцијата. |

| *Принцип П14.1.05* | |
|---|---|
| Одговорност за системските медиуми кои содржат информации кои не се за јавна употреба при пренос надвор од контролираните зони | • Контролирајте и одржувајте ја одговорноста за медиумите кои содржат информации кои не се од јавен карактер за време на транспортот надвор од контролираните области.<br>• Безбедносни методи на пакување и транспорт, како што се пакување без манипулации или курирски услуги со следење на безбедносниот синџир.<br>• Користете шифрирани комуникациски канали при електронски пренос на NPI.<br>• Креирајте записи на активности за транспорт на медиуми, вклучувајќи го испраќачот, примачот, датумот и начинот на транспорт.<br>• Секогаш кога можете препорачувајте силни механизми за криптографија. |
| Контролирање на начинот на користење на преносните медиуми како компоненти на систем | • Контролирајте ја употребата на отстранлив медиум на компонентата на системот со:<br>○ Воспоставување полиса која ја опишува прифатливата употреба на преносни медиуми, вклучувајќи видови медиуми, уреди и околности под кои е дозволена нивната употреба.<br>○ Спроведување технички контроли, како што се безбедносни решенија за крајна точка, за ограничување на употребата на неовластени преносни медиуми на компонентите на системот. |

## 14.2. Обработка на лични податоци и транспарентност

| Ниво | Безбедносни мерки |
|---|---|
| **1** | **14.2.1.** Идентификувајте ги и исполнете ги барањата за гарантирање и заштита на личните податоци и приватноста преку воспоставување безбедносна рамка за заштита на личните податоци.<br>**14.2.2.** Придржувајте се и соодветно имплементирајте го актуелниот Закон за заштита на личните податоци во Република Северна Македонија. |
| **2** | **14.2.3.** Креирајте процеси и технички контроли за идентификување, организирање, безбедно ракување, задржување и отстранување на личните податоци.<br>**14.2.4.** Прегледајте ја и ажурирајте ја политиката за заштита на податоци еднаш годишно или почесто во случај на потреба. |
| **3** | **14.2.5.** Нема специфични барања за Ниво 3. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| *Принцип П14.2.01* | |
|---|---|
| Интегрирана рамка за управување со заштитата на личните податоци | • Креирајте и воспоставете интегрирана рамка за управување со заштитата на личните податоци во согласност со важечките закони и регулативи и договорните барања.<br>• Креирајте и спроведете политика за заштита на лични податоци.<br>• Воспоставете пишани процедури и мерки кои обезбедуваат заштита на личните податоци во секојдневното работење. |

| | |
|---|---|
| | • Обезбедете примена на специфични услови за посебни/чувствителни категории на лични податоци.<br>• Идентификувајте и соодветно класифицирајте ги податоците во организацијата и мапирајте го нејзиниот тек низ различни процеси, системи и трети страни.<br>• Редовно прегледувајте и ажурирајте го пописот на податоците за да ги земете предвид промените во активностите и системите за обработка на податоци.<br>• Креирајте и одржувајте евиденција за активностите за обработка за да ја документирате секоја активност за обработка на лични податоци.<br>• Користете различни техники и алатки за пребришување на податоците и за намалување на ризиците кон личните податоци, како што се псевдоними, маскирање на податоците и шифрирање.<br>• Следете ги промените во регулаторната средина и соодветно ажурирајте ги политиките, процедурите и контролите за заштита на податоците за да се одржи усогласеноста. |
| Пристап до лични податоци | • Обезбедете регулирање и адекватно ограничување на пристапот до личните податоци преку имплементација на основата „потребно е да се знае“.<br>• Набљудувајте и снимајте каков било неовластен пристап до личните податоци.<br>• Поставете конкретни организациски и технички мерки за безбедно складирање и пренос на лични податоци. |
| ***Принцип П14.2.02*** | |
| Механизми за гарантирање на правата субјектите за податоци | • Воведете адекватно спроведување на механизми за гарантирање на правата на субјектите на податоците.<br>• Доставете известување до поединци за обработката на нивните лични податоци.<br>• Поставете дефинирани алатки или механизми со кои поединците ќе се согласат на обработката на нивните податоци пред нивното собирање, што го олеснува донесувањето одлуки при информирање на поединците.<br>• Поставете механизми за информирање на субјектите на податоците за нивните права, легитимни цели за обработка на нивните лични податоци или какви било трансфери на трети страни.<br>• Креирајте процес за справување со барањата за пристап на субјектите на податоците, вклучувајќи механизми за исправка, бришење и преносливост на податоците. |
| ***Принцип П14.2.03*** | |
| Релевантни обуки на вработените | • Организирајте стандардизирани обуки за заштита на личните податоци приспособени строго во согласност со доделените улоги и одговорности на вработените во однос на личните податоци и приватноста. |

## 15. РАЗУЗНАВАЊЕ ЗА САЈБЕР ЗАКАНИ

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **15.1.** Нема |
| **2** | **15.2.** Создавање на политики за собирање и консолидирање на разузнавачки информации за заканите.<br>**15.3.** Процедури за одговор на инцидентот кога се добиваат веродостојни разузнавачки информации за закани.<br>**15.4.** Спроведување на програма за подигање на свеста за заканите која вклучува способност за размена на разузнавачки информации за закани меѓу организациите. |
| **3** | **15.5.** Користење на сите стандардизирани протоколи (како STIX/TAXII) за автоматско споделување индикатори.<br>**15.6.** Воспоставете процеси за да се обезбеди навремено споделување на разузнавачки информации за закани.<br>**15.7.** Користете рамка за анализа на сериозноста и влијанието на заканата врз основа на добиените разузнавачки информации за закани.<br>**15.8.** Приспособување на безбедносните контроли врз основа на разузнавачките информации за закани.<br>**15.9.** Обезбедете интероперабилност со платформи за размена на разузнавачки информации за закани со други организации. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| *Принцип П15.01* | |
|---|---|
| Редовно мониторирање на надворешните закани со користење на разузнавачки информации | • Претплатете се на отворените и комерцијалните извори за разузнавачки информации за да останете информирани за најновите закани.<br>• Одржувајте снимен записи на разузнавачки информации за значајни закани собрани од различни извори, вклучително и безбедносни истражувачи, за да ги следите трендовите и моделите. |
| Учество во иницијативи за споделување на информации | • Учествувајте во Центрите за споделување и анализа на информации (ISAC) и иницијативи предводени од владата за размена на разузнавачки информации за заканите.<br>• Вклучете се во заеднички напори со индустриските партнери и владините агенции за справување со заедничките предизвици за сајбер безбедноста и ефективно споделување разузнавачки информации за заканите. |
| Споделување на информации за заканите со доверливи партнери | • Споделете разузнавачки информации за заканите што може да се преземат, како што се индикаторите за компромитирање (IOC), примероци од злонамерен софтвер и техниките за напад, со доверливи партнери.<br>• Соработувајте со слични организации за да ја подобрите свесноста за ситуацијата и да ја зајакнете одбраната од новите закани. |

| | |
|---|---|
| Воспоставување на безбеден и доверливи механизам за споделување на информации за заканите | • Воспоставете механизми и протоколи за безбедно и доверливо споделување разузнавачки информации за заканите.<br>• Поставете контроли за пристап и шифрирање за да се осигура дека чувствителните информации се заштитени и споделени само со овластени страни. |
| ***Принцип П15.02*** | |
| Верификација на изворот | • Потврдете го кредибилитетот и угледот на изворот што обезбедува разузнавачки информации за заканите.<br>• Оценете го досието на изворот и веродостојноста во доставувањето точни и навремени информации. |
| Крос-референцирање | • Направете вкрстување на разузнавачките информации за дојдовни закани со повеќе доверливи извори за да се потврди нивната точност и релевантност.<br>• Споредете ги информациите од различни извори за да идентификувате недоследности или несогласувања. |
| Анализа на контекст | • Анализирајте го контекстот за да ја согледате релевантноста на разузнавачките информации за заканите за специфичното опкружување и можните заканите врз безбедносната положба на организацијата.<br>• Утврдете го потенцијалното влијание на заканата врз средствата, операциите и безбедносната положба на организацијата. |
| Корелација на внатрешните податоци | • Поврзете ги дојдовните разузнавачки информации за заканите со внатрешните податоци и безбедносните настани за да ја процените нивната усогласеност со познатите закани и ранливости.<br>• Потврдете ја конзистентноста на разузнавањето со внатрешните согледувања во организацијата и извештаите за инциденти. |
| Експертски согледувања | • Вклучете експерти од областа (SMEs) или безбедносни аналитичари во прегледот и потврдувањето на дојдовните разузнавачки информации за заканите.<br>• Искористете ја нивната експертиза за да го процените кредибилитетот и релевантноста на разузнавањето врз основа на техничка анализа и знаење за доменот. |
| ***Принцип П15.03*** | |
| Стандардизација на формати и протоколи | • Прифатете и применете формати и протоколи на индустриски стандарди за размена на податоци за разузнавање од доменот на сајбер заканите со цел да се обезбеди интероперабилност со платформите на други организации.<br>• Користете формати како STIX (Structured Threat Information eXpression) и TAXII (Trusted Automated EXchange of Indicator Information) за беспрекорна интеграција. |
| API Интеграција | • Поставете програмибилни апликациски интерфејси (API) за да се олесни размената на разузнавачки податоци за закани помеѓу различни платформи. |

| | |
|---|---|
| | • Осигурете се дека апликациските програмибилни интерфејси (API) поддржуваат заеднички протоколи и механизми за автентикација за безбедна комуникација. |
| Партнерства за соработка | • Воспоставете партнерства за соработка со други организации и иницијативи за споделување информациите за заканите со цел за точно насочување на размената на разузнавачки информации меѓу организациите.<br>• Учествувајте во заедници и форуми за споделување специфични закани со цел поттикнување и одржување на интероперабилноста и колективните одбранбени напори. |
| ***Принцип P15.04*** | |
| Автоматизирано снабдување со закани | • Поставете автоматизирани процеси за собирање, анализа и ширење на ново идентификуваните закани од различни извори, вклучително и внатрешни системи за следење и надворешни извори.<br>• Користете платформи за разузнавање закани или системи за безбедносна информација и управување со настани (SIEM) за автоматизирање на собирањето и дистрибуцијата на информациите за закани. |
| Механизми за алармирање | • Поставите автоматизирани механизми за алармирање со цел навремено известување на релевантните засегнати страни за ново идентификуваните закани во реално време.<br>• Конфигурирајте приспособливи аларми врз основа на однапред дефинирани критериуми како што се сериозноста на заканата, релевантноста за организацијата и засегнатите средства. |

## 16. РАЗМЕНА НА ИНФОРМАЦИИ И ДОГОВОРИ

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **16.1.** Информирање на крајните корисници на комуникациските мрежи и услуги за одредени и значајни безбедносни инциденти кои можат да влијаат на нив. |
| **2** | **16.2.** Воспоставување на протоколи за споделување информации за заканите со други субјекти (т.е. организации од јавниот сектор / органи за спроведување на законот / организации од приватниот сектор / вашиот синџир на снабдување или други трети страни/итн.)<br>**16.3.** Поставување на решенија со технологија за заштита на информации и автоматско споделување.<br>**16.4.** Воспоставете и одржувајте информации за контакт со цел пријавување безбедносни инциденти (CIS) |
| **3** | **16.5.** Нема |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П16.01*** | |
|---|---|
| Информирање на крајните корисници на комуникациските мрежи и сервиси за специфичните и значајните безбедносни инциденти кои може да ги афектираат нив | • Јасна и разбирлива комуникација<br>○ При безбедносни инциденти комуницирајте на јасен и разбирлив начин, избегнувајќи технички речник што може да ги збуни крајните корисници.<br>○ Обезбедете активни совети за тоа како крајните корисници можат да се заштитат себеси и да ги намалат ризиците поврзани со идентификуваните закани.<br>• Обезбедете навремени известувања до крајните корисници за одреден и значаен безбедносен инцидент што може да влијае на мрежата или услугата што ја користат.<br>○ Користете повеќе канали за комуникација како што се е-пошта, СМС предупредувања и известувања во апликацијата, социјални медиуми за да обезбедите широк дофат. |
| ***Принцип П16.02*** | |
| Воспоставување на протоколи за размена на информации | • Развијте формални договори/протоколи со доверливи партнери, добавувачи и засегнати страни во кои ќе се наведат условите за споделување информации.<br>• Дефинирајте го опсегот на информациите што треба да се споделат, вклучително и барањата за класификација, чувствителност и ракување со податоци, за да се обезбеди доверливоста, интегритетот и достапноста.<br>• Наведете ги законските и регулаторните обврски за усогласеност, приватност и барањата за заштита на податоците во договорите за споделување информации за да се намалат ризиците и обврските. |
| ***Принцип П16.03*** | |
| Безбедни канали за комуникација | • Имплементирајте безбедни комуникациски канали, како што се шифрирана е-пошта, безбедносни протоколи за пренос на датотеки (SFTP)/FTPS, виртуелни приватни мрежи (VPN) и безбедносни платформи за размена на |

| | |
|---|---|
| | пораки, за безбедно да разменувате чувствителни информации.<br>• Конфигурирајте механизми за шифрирање, дигитални потписи и контроли за автентикација за да ја заштитите доверливоста, интегритетот и автентичноста на споделените информации за време на транзитот и складирањето.<br>• Поставете контроли за пристап и механизми за проверка на корисникот за да се ограничи пристапот до споделени информации врз основа на принципот на минимална привилегија и потреба да се знае. |

## 17. БЕЗБЕДНОСНИ ПОЛИТИКИ И ПРОЦЕДУРИ

| НИВО | Безбедносни мерки |
|---|---|
| **1** | **17.1.** Креирање, воспоставување и комуницирање на политика за безбедност на информации (ISP) во согласност со важечките законски, статутарни и регулаторни барања.<br>**17.2.** Воспоставување и документирање оперативни процедури за капацитети за обработка на информации. |
| **2** | **17.3.** Дефинирање, објавување и комуницирање на понатамошни соодветни политики за одредена тема.<br>**17.4.** Редовен преглед на политиката за безбедност на информациите и останатите политики во планирани интервали и во случај кога ќе се случат значителни промени.<br>**17.5.** Преглед и оцена на оперативните процедури во планирани интервали и во случај кога ќе се случат значителни промени.<br>**17.6.** Дефинирање на барањата за управување со безбедноста на информациите споделени со надворешни страни. |
| **3** | **17.7.** Преглед и периодично ажурирање (најмалку еднаш годишно или кога е потребно) на безбедносните планови за организациските информациски системи.<br>**17.8.** Ако активноста на владината организација е критична за државата, националната безбедност или јавната безбедност, или ако обработува голема количина на критични информации кои не се од јавен карактер, тогаш се препорачува да се имплементира систем за управување со информациска безбедност - ISMS. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***Принцип П17.01*** | |
|---|---|
| Политика за безбедност на информации | • Обезбедете политика за безбедност на информациите кои треба да бидат јасни, прецизни и конзистентни.<br>• Основните елементи на интернет провајдерот:<br>○ цел,<br>○ опсег,<br>○ улоги и одговорности,<br>○ посветеност на управувањето,<br>○ координација меѓу организациските субјекти и<br>○ усогласеност.<br>• Следете го и оценувајте го спроведувањето на политиките на редовна основа, најмалку еднаш годишно, или во случаеви кога се случуваат значителни промени.<br>• Ревидирајте ја безбедносната политика по инциденти.<br>• Организирајте различни активности за да го запознаете клучниот персонал за безбедносната политика.<br>• Назначете службеник или член на персоналот да раководи со развојот, документацијата и споделување на информации со интернет провајдерот. |
| ***Принцип П17.02*** | |
| Оперативни процедури | • Создавање и спроведување на Оперативни процедури за да се олесни спроведувањето на безбедносната политика и поврзаните безбедносни контроли.<br>• Оперативните процедури треба да вклучуваат најмалку:<br>○ инструкции за инсталирање, конфигурирање и ажурирање системи и софтвер, |

| | |
|---|---|
| | ○ правила за евидентирање, следење и справување со грешки или исклучоци, вклучително и ограничувања за употреба на системски алатки,<br>○ рестартирање и обновување на системот во случај на дефект (најмалку еден годишно), усогласеноста на интернет провајдерот со овој стандард и другите законски прописи треба да се провери.<br>• Преглед и оценување на Оперативните процедури годишно или во случај кога се случуваат значителни промени. |
| ***Принцип П17.03*** | |
| Планови за безбедност | • Креирање на безбедносни планови со контроли за информациските системи и правила на однесување за поединци кои пристапуваат до информациските системи.<br>• Безбедносните планови треба да бидат конзистентни и во согласност со интернет провајдерот и оперативните процедури.<br>• Безбедносните планови треба да се креираат во тесна соработка со раководството на организацијата. |
| ***Принцип П17.04*** | |
| Ревизии | • Извршете внатрешната ревизија следејќи ги најдобрите практики и водечките примери.<br>• Внатрешната ревизија може да ја вршат вработени во јавни институции со соодветна обука или одобрени трети лица.<br>• Документирајте ги и чувајте ги сите извештаи од извршените внатрешни и надворешни ревизии. |
| ***Принцип Р17.05*** | |
| Меѓународни стандарди | • Користете меѓународни стандарди како што е ISO/IEC 27001 [ISO27001] за имплементација на систем за управување со информациска безбедност - ISMS. |

## 18. ЗАШТИТА НА ФИЗИЧКАТА И ЖИВОТНАТА СРЕДИНА (ПЛАН ЗА ВОНРЕДНА СОСТОЈБА)

| *НИВО* | *БЕЗБЕДНОСНИ МЕРКИ* |
|---|---|
| **1** | **18.1.** Спроведување на сеопфатни проценки на ризик за да се поделат управуваните области во посебни безбедносни зони приспособени на специфични безбедносни потреби врз основа на идентификуваните ризици.<br>**18.2.** Строго контролирање на пристапот до безбедносните зони, давајќи им пристап само на овластени лица со легитимна основа.<br>**18.3.** Воспоставете мерки за контрола на пристапот за ограничување на физичкиот пристап до организациски системи, опрема и оперативни средини.<br>**18.4.** Обезбедете пристап на овластени лица врз основа на службени должности, редовно прегледувајќи ги и ажурирајќи ги дозволите за пристап доколку е потребно.<br>**18.5.** Имплементирајте годишна основна обука за физичка безбедност на вработените за да ја зголемите свесноста за безбедносните ризици и најдобрите практики, покривајќи теми како што се препознавање сомнителни активности, пријавување безбедносни инциденти и следење процедури за контрола на пристап. |
| **2** | **18.6.** Одржувајте сеопфатни записи за сите активности со физички пристап во објектите, запишувајќи детали како датум, време, локација и индивидуален идентитет, обезбедувајќи одговорност и овозможувајќи форензичка анализа.<br>**18.7.** Активно помагајте и следете ги активностите на посетителите во просториите за да се обезбеди безбедност и усогласеност со процедурите за пристап, распоредувајќи безбедносен персонал или системи за надзор за подобрување на севкупните безбедносни мерки. |
| **3** | **18.8.** Спроведувајте сеопфатни контроли и процедури за управување со уредите за физички пристап, како што се картички, клучеви, PIN кодови и картички за пристап за безбедносен пристап до објектите и чувствителните области.<br>**18.9.** Спроведете строги заштитни мерки за заштита на информациите кои не се од јавен карактер (NPI) и вршете обработка на алтернативни работни места, како што се центрите за опоравување после катастрофи, заштитувајќи ги критичните податоци од неовластен пристап или откривање.<br>**18.10.** Обезбедете сеопфатна обука за физичка безбедност на сите вработени, вклучувајќи го и безбедносниот персонал, покривајќи напредни теми како што се откривање закани, процедури за одговор при итни случаи и протоколи за справување со инциденти, осигурувајќи се дека персоналот е добро подготвен за ефективно да одговори на различните безбедносни предизвици. |

Не ограничувајќи се само на овие принципи - за да се применат овие безбедносни мерки, треба да се земат предвид следните принципи:

| ***ПРИНЦИП П18.01*** | |
|---|---|
| Детален дизајн на безбедносните зони | • Креирајте ги безбедносните зони прецизно за да се спротивставите на очекуваните сценарија за напад.<br>• Имајте за цел да ги забавите акциите на потенцијалните напаѓачи и да обезбедите соодветно време за реакција. |
| Фокусирање на елиминација на ранливостите | • Креирајте ја секоја зона за да се фокусира на елиминирање на ранливостите и зајакнување на одбраната врз основа на сеопфатни проценки на ризикот. |
| Нагласување на безбедносните мерки | • Поставете безбедносни мерки кои се интензивираат кога потенцијалните напаѓачи се приближуваат до зоните кои ја штитат критичната организациска инфраструктура.<br>• Имајте за цел да се одвратат или одложат нападите, овозможувајќи навремена реакција и избегнување на заканите. |
| ***Принцип П18.02*** | |
| Сеопфатна обука за безбедност | • Проширете го барањето за безбедносна свест и обука на сите поединци кои пристапуваат до просториите на организацијата.<br>• Осигурете се дека напорите за обука ги покриваат безбедносните протоколи и улогите на поединците во одржувањето на безбедна средина. |
| Воспоставување на правила и процедури за пристап | • Наведете конкретни упатства за влегување, излегување и движење во безбедносните зони за да обезбедите доследно придржување до безбедносните протоколи.<br>• Документирајте ги исклучоците за одредени поединци или услуги со јасни упатства за имплементација. |
| Основна обука за сите вработени | • Обезбедете основна обука за безбедност која опфаќа суштински теми за подготвеност и одговор на кризи за сите вработени.<br>• Покријте различни аспекти на безбедноста и подготвеност за итни случаи, вклучувајќи идентификација на закани, безбедносни протоколи и процедури за итна евакуација. |
| ***ПРИНЦИП П18.03*** | |
| Одржување на записи за ревизија | • Водете записи за ревизија на активностите за физички пристап најмалку 12 месеци.<br>• Обезбедете олеснување на ретроспективна анализа и истрага за безбедносни инциденти преку сеопфатни записи за ревизија. |
| ***ПРИНЦИП П18.04*** | |
| Опсег на технологии и протоколи | • Поставете физички безбедносни мерки кои опфаќаат низа технологии и протоколи за заштита на организациски средства и инфраструктура.<br>• Вклучете персонал, бариери, системи за контрола на пристап, надзор, аларми, откривање пожар, откривање |

| | |
|---|---|
| | поплави, климатизација и иницијативи за подигање на свеста на вработените. |
| Регистрација и индивидуализација на пристапните уреди | • Регистрирајте и персонализирајте ги уредите за физички пристап, како што се беџови или клучеви, за да ја подобрите одговорноста и следење.<br>• Означете го или нумерирајте го секој уред за лесна идентификација и следење. |
| Документирање на правилата и протоколите за пристап | • Дефинирајте правила за документи со кои се регулира складирањето, издавањето и размената на уредите за пристап за да се обезбеди конзистентност и одговорност.<br>• Јасно дефинирајте ги процедурите за издавање картички или клучеви, периодични промени на кодот и надзор од посетители. |
| Надгледуван пристап за посетители | • Осигурете се дека посетителите добиваат пристап до објекти под надзор на овластен персонал во текот на времетраењето на нивната посета.<br>• Обезбедете одговорност и надзор над активностите на посетителите во заштитените простории. |
| Безбедносни карактеристики за пристапните ознаки | • Поставете безбедносни елементи во картичките за пристап за да спречите манипулација или фалсификување, зголемувајќи го непромеливоста на податоците и доверливост.<br>• Поставете информации за контакт на картичките за пријавување на изгубени картички на овластен безбедносен персонал. |
| ***ПРИНЦИП П18.05*** | |
| Развој на процедури за зачувување на резервни копии | • Воспоставете детални процедури за правење резервна копија и тестирање на податоците, софтверот и резервната копија на податоци од системот, земајќи ги предвид сите релевантни, нови и променети податоци.<br>• Наведете ја фреквенцијата на извршување, времетраењето на складирањето и типот на резервна копија врз основа на природата на системот, значењето на податоците и зачестеноста на промените. |
| Типови и методи за зачувување на резервни копии | • Користете различни методи за резервна копија, како што се офлајн, офлајн и онлајн резервни копии за да се обезбеди сеопфатна заштита на податоците.<br>• Изберете типови на резервни копии и синтетички целосни резервни копии врз основа на процесите на анализа на ризик и копирање податоци.<br>• Воспоставете процедури за креирање и складирање резервни копии на надворешни локации надвор од капацитетите на организацијата за да се намалат ризиците од прекин или дефект на инфраструктурата. |
| Безбедно зачувување и шифрирање | • Шифрирајте и складирајте резервни копии во посебни простори во мрежата на организацијата за да се обезбеди ограничен пристап и без интернет конекција.<br>• Редовно тестирајте ги процесите за резервна копија и обновување за да се обезбеди точност и ефективност, |

| | |
|---|---|
| | особено по значителни промени во архитектурата на ИКТ.<br>• Спроведување на вишок во капацитетите за обработка на информации, вклучително и критичните мрежни уреди и сервери, за да се исполнат барањата за достапност и да се обезбеди непречено работење. |
| Подготовка на предупредување и комуникациски планови | • Организирајте ја структурата за одговор со цел олеснување на брзите и координирани акции за време на кризни ситуации, обезбедувајќи ефективна комуникација и донесување на одлуки.<br>• Подгответе планови/процедури за предупредување и комуникација за да се дистрибуираат навремени информации и инструкции до релевантните засегнати страни за време на итни случаи. |
| Креирање и тестирање на планови за работа при вонредни состојби | • Креирајте детални планови и процедури за континуитет на деловното работење, наведувајќи ги чекорите за обновување и повратак на критичните процеси и ресурси.<br>• Редовно тестирајте ги плановите и процедурите за континуитет на бизнисот за да ја потврдите ефективноста и да ги идентификувате областите за подобрување.<br>• Воспоставете механизми за континуирано подобрување за да ги прегледате и подобрите стратегиите, плановите и способностите за одговор за континуитет на бизнисот врз основа на повратни информации и научени лекции од тестирањето и инцидентите од реалниот свет. |

# Прилог 1. Мапирање на безбедносните контроли со меѓународните стандарди (NIST, ENISA, NIS2, ISO, CIS, NCSA)

| Стандард | ISO/IEC 27001:2022 | ISO/IEC 27002:2022 | ENISA | NIS2 | NIST SP 800-53 | CIS Controls v8 | NCSA |
|---|---|---|---|---|---|---|---|
| **1. Управување со сметки и контрола на пристап** | Annex A.9 (Access Control) | Section 9 (Access Control) | Access Control Management | Articles 19-21 (Risk Management) | Access Control (AC) | Control 6 (Access Control Management), Control 16 Account Monitoring | Section 3 (Access Control Practice) |
| **2. Контрола на каталог на средства (Хардвер и софтвер)** | Annex A.8 (Asset Management) | Section 8 (Asset Management) | Asset Inventory | Articles 19-21 (Governance & Risk Management) | CM-8 (System Component Inventory) | Control 1 (Inventory of Assets), Control 2 (Software Assets) | Section 4 (Asset Inventory) |
| **3. Безбедносни конфигурации и управување со закрпи (средства)** | Annex A.12 (Operations Security) | Section 12 (Secure Configuration) | Secure Configuration Guidelines | Articles 19-21 (Technical Measures) | CM (Configuration Management) | Control 4 (Secure Configuration), Control 7 (Vulnerability Management) | Section 4 (Patch & Configuration Management) |
| **4. Управување со ранливости и пенетрацисko тестирања** | Annex A.12.6 (Vulnerability Management) | Section 12.6 (Technical Vulnerability Management) | Vulnerability and Patch Management | Article 19 (Risk Management) | RA-5 (Vulnerability Monitoring) | Control 7 (Vulnerability Management) | Section 4 (Penetration Testing & Vulnerability Scanning) |
| **5. Управување и ревизија на записи** | Annex A.12.4 (Logging and Monitoring) | Section 12.4 (Logging and Monitoring) | Logging & Monitoring Practices | Article 19 (Risk Management) | AU (Audit and Accountability) | Control 8 (Audit Log Management) | Section 7 (Audit Logging) |
| **6. Заштита на е- пошта и прикажувачи** | Annex A.13 (Communications Security) | Section 13 (Communications Security) | Email and Web Security | Articles 19-21 (Technical Measures) | SC-7 (Boundary Protection), SC-18 (Cryptographic Protection) | Control 9 (Email & Browser Protection) | Section 8 (Email and Web Protection) |

| Стандард | ISO/IEC 27001:2022 | ISO/IEC 27002:2022 | ENISA | NIS2 | NIST SP 800-53 | CIS Controls v8 | NCSA |
|---|---|---|---|---|---|---|---|
| **7. Одбрана од злонамерен софтвер и анализа** | Annex A.12.2 (Protection Against Malware) | Section 12.2 (Malware Protection) | Malware Protection and Incident Response | Articles 19-21 (Technical Measures) | SI-3 (Malware Protection) | Control 10 (Malware Defenses) | Section 9 (Malware Analysis & Defense) |
| **8. Управување со мрежна инфраструктура** | Annex A.13 (Network Security) | Section 13 (Network Security) | Network Security Management | Articles 19-21 (Technical Measures) | SC (System and Communications Protection) | Control 11 (Network Infrastructure Management) | Section 10 (Network Infrastructure Security) |
| **9. Мониторирање и одбрана на мрежа** | Annex A.13.1 (Network Security) | Section 13.1 (Network Security) | Network Monitoring and Detection | Articles 19-21 (Risk Management) | SC-7 (Boundary Protection), AU-12 (Audit and Monitoring) | Control 12 (Network Monitoring) | Section 10 (Network Defense) |
| **10. Обука за безбедносна свест и вештини** | Annex A.7 (Human Resource Security) | Section 7.2 (Awareness and Training) | Security Awareness and Education | Article 19 (Risk Management) | AT (Awareness and Training) | Control 14 (Security Awareness) | Section 5 (Security Awareness) |
| **11. Управување на даватели на услуги (и добавувачи /трета страна)** | Annex A.15 (Supplier Relationships) | Section 15 (Supplier Security) | Supply Chain Security | Article 24 (Supply Chain Management) | SA (System and Services Acquisition) | Control 15 (Service Provider Management) | Section 6 (Third-Party Risk Management) |
| **12. Безбедно тестирање и преглед на код** | Annex A.14 (System Acquisition, Development, and Maintenance) | Section 14 (Development Security) | Secure Development and Testing | Article 19 (Risk Management) | SA-11 (Developer Security Testing and Evaluation) | Control 16 (Application Software Security) | Section 11 (Secure Development and Testing) |
| **13. Одговор при инциденти и поврат на податоци** | Annex A.16 (Incident Management) | Section 16 (Incident Management) | Incident Response Planning | Article 21 (Incident Response) | IR (Incident Response) | Control 17 (Incident Response) | Section 12 (Incident Response & Recovery) |
| **14. Заштита на податоците и приватност** | Annex A.18 (Compliance) | Section 18 (Compliance) | Data Protection Guidelines | Article 22 (Data Protection) | MP (Media Protection), PT (Privacy) | Control 13 (Data Protection) | Section 13 (Data Privacy & Protection) |

| Стандард | ISO/IEC 27001:2022 | ISO/IEC 27002:2022 | ENISA | NIS2 | NIST SP 800-53 | CIS Controls v8 | NCSA |
|---|---|---|---|---|---|---|---|
| **15. Разузнавање за сајбер закани** | N/A | N/A | Threat Intelligence Management | N/A | SI-4 (Information System Monitoring) | N/A | N/A |
| **16. Размена на информации и договори** | Annex A.15 (Supplier Relationships) | Section 15 (Supplier Security) | Information Sharing Guidelines | Articles 19-21 (Risk Management) | CA (Security Assessment and Authorization) | N/A | Section 14 (Information Sharing) |
| **17. Безбедносни политики и процедури** | Annex A.5 (Information Security Policies) | Section 5 (Information Security Policies) | Policy and Strategy Management | Articles 19-21 (Governance) | PL (Planning) | Control 1 (Establish Security Program) | Section 1 (Security Policy) |
| **18. Заштита на физичката и животната средина (план за вонредна состојба)** | Annex A.11 (Physical and Environmental Security) | Section 11 (Physical and Environmental Security) | Physical Security Guidelines | Articles 19-21 (Technical Measures) | PE (Physical and Environmental Protection) | Control 13 (Data Protection) | Section 15 (Physical & Environmental Security) |

# Референци

| ОДГОВОРНО МИНИСТЕРСТВО/БРОЈ НА СТАНДАРД | ИМЕ И ТИП НА ДОКУМЕНТ |
|---|---|
| **МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА** | **Стратегиски документи:**<br>Стратегија за сајбер безбедност (2018-2022)<br>Стратегија за сајбер безбедност (2023-2027)*<br>Национална краткорочна ИКТ стратегија (2016-2017)<br>Национална ИКТ стратегија (2023-2027)**<br>**Закони и подзаконски акти:**<br>Закон за безбедност на мрежи и информатички системи и дигитална трансформација***<br>Закон за Електронско управување и електронски сервиси<br>Закон за електронски документи, електронска идентификација и сервиси за доверба<br>Закон за електронски комуникации<br>Закон за воспоставување на македонска академска мрежа за истражување<br>Закон за архивски материјал<br>Стандарди за квалитет на податоци во системите на државните институции<br>Правилник за стандардите и правила за безбедност на ИТ системи кои се користат во телата на јавната администрација за електронска комуникација<br>Упатство за мониторирање и управување со инциденти кои се однесуваат на ИТ безбедноста<br>Упатства за реализација на анализа на ризик и управување со ризик |
| **МИНИСТЕРСТВО ЗА ОБРАНА** | **Стратешки документи:**<br>Стратегија за сајбер одбрана (2020)<br>Стратегија за градење на еластичност и справување со хибридни закани (2021-2025)*<br>**Законски и подзаконски акти:**<br>Закон за критична инфраструктура<br>Закон за обрана |
| **МИНИСТЕРСТВО ЗА ВНАТРЕШНИ РАБОТИ** | **Стратешки документи:**<br>Стратегија за сајбер криминал (2018-2022)<br>Стратегија за сајбер криминал<br>**Законски и подзаконски акти:**<br>3.3 Закон за набљудување на комуникации |
| **ДИРЕКТОРАТ ЗА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ** | **Законски и подзаконски акти:**<br>5.1 Закон за класифицирани информации<br>Уредба за физичка безбедност на класифицирани информации<br>Уредба за административна безбедност на класифицирани информации<br>Уредба за лична безбедност<br>Уредба за индустриска безбедност на класифицирани информации |

| | |
|---|---|
| | Уредба за информациска безбедност на класифицирани информации |
| **АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ** | **Законски и подзаконски акти:**<br>Закон за заштита на лични податоци<br>Закон за ратификација на Протоколот за усвојување на Конвенцијата за заштита на личноста при автоматско обработка на податоци<br>Дополнителни протоколи на Конвенцијата за заштита на личности при автоматско обработка на податоци во врска со тела за надзор и пренесување на податоци преку граница<br>Правилник за заштита на процесирачки податоци<br>Правилник за содржината и формата на актот за начинот на вршење на видеонадзор<br>Правилник за измена и дополна на Правилник за содржината и формата на актот за начинот на вршење на видеонадзор<br>Правилник за содржината на анализата на целта, односно целите за која се поставува видеонадзорот и извештајот од извршена периодична оценка на постигнатите резултати од системот за вршење видеонадзор<br>Правилник за трансфер на податоци<br>Правилник за процесот на анализа на влијанието на заштитата на личните податоци<br>Правилник за формата и содржината на барањето за утврдување на прекршување на одредбите од законот за заштита на личните податоци<br>Правилник за начинот на известување за нарушување на безбедноста на личните податоци<br>Правилник за известување за обработка на лични податоци со висок ризик<br>Одлука за утврдување на стандардни договорни клаузули за пренос на лични податоци во трети земји |
| **МИНИСТЕРСТВО ЗА ПРАВДА**<br>**КРИВИЧЕН СУД**<br>**КАНЦЕЛАРИЈА НА ЈАВЕН ОБВИНИТЕЛ** | Кривичен законик |
| **МИНИСТЕРСТВО ЗА ПРАВДА**<br>**КРИВИЧЕН СУД**<br>**КАНЦЕЛАРИЈА НА ЈАВЕН ОБВИНИТЕЛ** | Закон за кривична постапка |
| **МИНИСТЕРСТВО ЗА ПРАВДА**<br>**ЦИВИЛЕН СУД** | Закон за цивилна постапка |
| **АГЕНЦИЈА ЗА АДМИНИСТРАЦИЈА** | Закон за генерална административна постапка |
| **МИНИСТЕРСТВО ЗА ПРАВДА** | Закон за литигација |

| | |
|---|---|
| **ДРЖАВЕН ЗАВОД ЗА СТАТИСТИКА** | Закон за државна статистика |
| **[800-171]** | NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020 |
| **[ISO27000]** | ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary |
| **[ISO27002]** | ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls |
| **[ISO27001]** | ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements |
| **[ISO27005]** | ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks |
| **[ISO19011]** | ISO 19011:2018 Guidelines for auditing management systems |
| **[ISO17021]** | ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements |
| **[ISO31000]** | ISO 31000:2018 Risk management – Principles and guidelines |
| **[ISO22301]** | ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements |
| **[ENISA-1]** | ENISA Technical guidelines for implementation of minimum-security measures for Digital Service Providers, December 2016 |
| **[ENISA-2]** | ENISA Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a, Version 2.0, October 2014 |
| **[FICIC]** | Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, April 16, 2018, |