

# ПОЛИТИКА

## ИНФОРМАЦИОННА СИГУРНОСТ

### 79. СУ Индира Ганди – гр. София

Съдържание I. Въведение.....	2
II. Цел .....	2
III. Организиране на сигурност на информацията .....	2
IV. Сигурност на човешките ресурси.....	2
V. Управление на активите.....	2
VI. Контрол на достъпа.....	4
VII. Криптография.....	4
VIII. Физическа сигурност и сигурност на заобикалящата среда.....	4
IX. Сигурност на работата.....	6
X. Сигурност на комуникациите .....	6
XI. Взаимоотношения с доставчици .....	6
XII. Управление на инциденти със сигурността на информацията .....	7
XIII. Съответствие .....	7
XIV. Прегледи на сигурността на информацията .....	8

## **I. Въведение**

Политиката за информационна сигурност въвежда механизми за контрол при обработване на лични данни и изпълнение на всички изисквания на Регламент (ЕС) 2016/679 (Общ регламент относно защита на данните), националното и правото на ЕС.

## **II. Цел**

Настоящата политика определя насоката на действие и поддържане на управлението на сигурността на информацията в съответствие с действащите нормативни актове и добри практики.

## **III. Организиране на сигурност на информацията**

1. Вътрешна организация – 79. СУ Индира Ганди установява управленска рамка за въвеждане и контрол върху реализирането и оперирането със сигурността на информацията.

1.1. Роли и отговорности по сигурност на информацията – за сигурността на информацията в училището ще отговаря Директорът на 79. СУ Индира Ганди .

1.2. Разделяне на задълженията – всеки служител има определени задължения, на базата на които се определят правата на достъп до лични данни.

1.3. Контакт с оторизирани органи – контакт с оторизирани органи осъществява единствено директорът на 79. СУ Индира Ганди и Длъжностното лице по защита на данните.

### **2. Мобилни устройства и работа от разстояние**

Въвеждат се мерки за контрол и сигурност при работа от разстояния и ползване на мобилни устройства (преносими компютри). Всички мобилни устройства следва да осъществяват достъп до интернет в самостоятелно обособена за целта точка за достъп. Тя не трябва да бъде част от локалната вътрешна мрежа на организацията. Следва да разполага с отделна мрежа и да няма възможност за достъп до основната мрежа на организацията. Всички мобилни устройства трябва да разполагат със софтуер за криптиране на информацията и да бъде извършена процедурата по пълно криптиране на твърдия диск.

## **IV. Сигурност на човешките ресурси**

1. Преди наемане на работа - да се гарантира, че служители и доставчици разбират своите отговорности и са подходящи за ролите, които ще изпълняват.

1.1. Подбор на ръководни кадри и служители имащи достъп до лични данни – трябва да бъде извършвано проучване за проверка на биографичните данни на всички кандидати за наемане на работа в съответствие с нормативни актове и етика и съобразно изискванията, свързани с дейността и класификацията на информацията, до която имат достъп, и предполагаемите рискове.

1.2. Срокове и условия при сключване на договори - договорните споразумения със служителите и доставчиците трябва да определят техните отговорности и отговорностите на организацията по отношение на сигурността на информацията. Длъжностната характеристика може да бъде използвана да се документират (опишат) отговорностите и ролите по сигурността. Отговорностите и ролите по сигурността на хора, които не взимат участие в процеса на назначаването, извършвано от институцията, например нает персонал от трети организации, трябва също да бъдат ясно дефинирани и обяснени.

2. По време на работа - да се гарантира, че служителите и доставчиците са запознати и изпълняват своите отговорности по отношение на сигурността на информацията.

2.1. Отговорности на ръководството - ръководството трябва да изисква от служителите и доставчиците да прилагат мерките за сигурност в съответствие с установените политики и процедури на организацията.

2.2. Осъзнаване, образование и обучение по сигурност на информацията - в съответствие със своите служебни функции всички служители на организацията и, където е уместно, доставчиците получават подходящо обучение с цел осъзнаване и редовно актуализиране на знанията по политиките и процедурите на организацията за информационна сигурност и обработка на лични данни.

2.3. Дисциплинарен процес - за служители, извършили нарушение по отношение на сигурността на информацията, съществува дисциплинарен процес.

3. Прекратяване или промяна на трудовите отношения – защитават се интересите на организацията като част от процеса за промяна или прекратяване на трудовите правоотношения.

4. Отговорности при прекратяване или промяна на трудовото правоотношение - отговорностите и задълженията по отношение на сигурността на информацията при прекратяване или промяна на трудовото правоотношение са определени, оповестени на служителя или доставчика и са приведени в действие. При напускане на служител, обработващ лични данни, се предприемат действия по ограничаване на достъпа му до системи обработващи лични данни, както и физическия му достъп до помещения, в които се съхраняват лични данни. Отговорността за това носи Директорът на училището. Трябва да бъдат сменени всички общодостъпни пароли, които се използват от много служители – пароли за Wi-Fi и други еднотипни пароли.

## **V. Управление на активите**

1. Отговорност за активите – идентифицират се активите на организацията и се определят съответните отговорности за защитата им.

1.1. **Опис на активите** - всички активи, свързани с информационните средства и средствата за обработване на информация, са ясно идентифицирани и на тези активи бива съставен и поддържан опис. Създава се специален регистър, който се актуализира постоянно.

1.2. Притежание на активи - В описане се посочват единствено притежаваните от **79. СУ Индира Ганди** активи.

1.3. Допустимо използване на активи – допустимо използване на информация и активи, свързани с информацията и средствата за обработване на информация е документирано и описано в длъжностната характеристика на съответния служител.

1.4. Връщане на активи - всички служители и потребители от трета страна при прекратяване на тяхното трудово правоотношение, договор или споразумение трябва да върнат всички употребявани от тях активи на организацията.

2. Работа с информационни носители - да се предотврати неотризирано разкриване, изменение, премахване или разрушаване на информация, съхранявана върху носители.

2.1. Управление на сменяеми външни носители – използването на сменяемите носители е силно ограничено. Извършва се мониторинг какви сменяеми носители се използват и каква информация се копира. Трябва да се използва специализиран софтуер за управление и мониторинг против изтичане на лични данни и чувствителна информация. Информацията върху сменяемите външни носители трябва да бъде криптирана чрез специализиран софтуер.

2.2. Унищожаване на носители – ненужните и повредени носители се унищожават по сигурен начин, като се използват стандартизирани процедури за унищожаване на информация.

2.3. Пренасяне на физически носители - по време на транспортиране носителите, съдържащи информация, са защитени срещу неотризиран достъп, използване не по

предназначение или подправяне. За целта информацията върху външните носители трябва да бъде криптирана чрез специализиран софтуер.

## **VI. Контрол на достъпа**

1. Изисквания за дейността за контрол на достъпа – ограничен е достъпът до информацията и средствата за обработване на информация.

1.1. Контрол на достъпа – съществува контрол на достъпа по отношение защитата на лични данни и са дефинирани ясни права и отговорности по отношение на достъпа и обработка на лични данни. Препоръчва се контрола на достъпа да се осъществява чрез специализирани средства, които да контролират достъпа.

1.2. Достъп до мрежи и мрежови услуги - на потребителите е осигурен достъп само до тези мрежи и мрежови услуги, за които те са изрично оторизирани да използват. Определя се с длъжностната характеристика за всеки служител.

2. Управление на достъпа на потребителите - да се гарантира оторизиран достъп на потребителите и да се предотврати неоторизиран достъп до системи и услуги.

2.1. Регистрация и прекратяване на регистрация на потребители – за всеки служител се създават потребители с дефинирани права за достъп. Потребителят може да бъде част от група, която също трябва да бъде с дефинирани права за достъп до определена информация. Потребителите нямат право да достъпват информация, която не касае преките им задължения и отговорности.

2.2. Осигуряване на достъп на потребители – системният администратор осигурява достъп на потребителите до съответната информация или група съгласно длъжностната характеристика на служителя.

2.3. Преглед на правата за достъп на потребителите – собствениците на активи трябва да преглеждат правата за достъп на потребителите през редовни интервали.

2.4. Отнемане или коригиране на права за достъп - правата за достъп на всички служители или потребители от трета страна до информацията и до средствата за обработване на информация трябва да бъдат отнети при прекратяване на трудовото правоотношение, договор или споразумение или коригирани при настъпване на промяна.

3. Отговорности на потребителите – потребителите се държат отговорни за защита на тяхната информация и автентификация.

4. Контрол на достъпа до системи и приложения - да се предотврати неоторизиран достъп до системи и приложения.

4.1. Ограничаване на достъпа до информация – ограничен е достъпът до информация и функциите на приложните системи в съответствие с длъжностната характеристика на служителя.

4.2. Система за управление на пароли - паролите трябва да бъдат интерактивни и да осигуряват качество и надеждност. Трябва да са минимум 8 символа, да съдържат една главна буква, малки букви, една цифра и поне един специален символ. Паролите не се записват в браузърите. Може да се използва надежден специализиран софтуер за управление на паролите. Добра практика е паролите да се сменят от потребителите на всеки 6 месеца.

4.3. Използване на привилегировани обслужващи програми - използването на обслужващи програми, които биха могли да преодолеят механизмите за контрол на системата и приложенията, трябва да бъде ограничено и строго контролирано.

## **VII. Криптография**

1. Криптографски механизми за контрол - да се защитят поверителността, достоверността и/или целостта на информацията чрез правилно и ефикасно използване на криптография.

1.1. Използване на криптографски механизми за контрол – препоръчително е информацията да бъде защитена чрез софтуер за криптиране, както и да бъде извършено

пълно криптиране на диска с цел да се осигури защита на информацията и достъп от неоторизирани лица.

1.2. Управление на ключове – ключовете трябва да бъдат управлявани чрез специализиран сървър за управление и контрол.

### **VIII. Физическа сигурност и сигурност на заобикалящата среда**

1. Сигурни зони - да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на организацията.

1.1. Граници за физическа сигурност - за защита на зони, които съдържат или чувствителна, или критична информация и средства за обработване на информация, се определят и използват граници за сигурност.

1.2. Механизми за контрол на физическо влизане – добра практика е сигурните зони да бъдат защитени със съответни механизми за контрол на влизане, за да се гарантира, че само оторизираният персонал има разрешен достъп.

1.3. Осигуряване на офиси, зали и съоръжения - трябва да бъде проектирана и приложена физическа защита за офиси, зали и съоръжения.

1.4. Защита от външни заплахи и заплахи от околната среда - трябва да бъде проектирана и приложена физическа защита от природни бедствия, злонамерени атаки или инциденти.

1.5. Работа в сигурни зони – трябва да се дефинират служителите, които имат достъп до помещенията, които са определени за сигурна зона.

2. Устройства - да се предотвратят загуби, повреди, кражби или излагане на риск на активите и прекъсване на дейностите на институцията.

2.1. Устройствата са разположени и защитени, така че да се намалят рисковете от заплахи и опасности от околната среда и възможности за неоторизиран достъп. Сървърите трябва да бъдат поставени в специални обособени сървърни помещения, които да са с подходяща климатизация и вентилация. През помещенията не трябва да минават канализационни тръби или тръбни водни трасета. Помещенията трябва да разполагат с противопожарна система. Достъпът до помещенията трябва да бъде силно ограничен.

2.2. Поддържащи комунални системи - устройствата трябва да бъдат защитени от повреди в електрозахранването и други разриви, предизвикани от откази в поддържащите комунални системи. Сървърите трябва да разполагат с онлайн UPS за резервиране на захранването.

2.3. Сигурност на окабеляването - окабеляването за електрозахранване и телекомуникации, носещо данни или поддържащо информационни услуги, трябва да бъде защитено от подслушване, смущения или повреда.

2.4. Изнасяне на собственост и активи - устройства, информация или софтуер не се изнасят извън организацията без предварително разрешение.

2.5. Сигурност на устройства и активи извън помещенията - сигурността трябва да бъде прилагана и към активи, които са извън организацията, като се отчитат различните рискове при работа извън помещенията на организацията.

2.6. Сигурно унищожаване или повторно използване на устройства - всички елементи на устройство, съдържащо запамятаващи носители, са проверявани, за да се гарантира, че всякакви чувствителни данни и лицензиран софтуер са премахнати или сигурно презаписани преди унищожаването или повторното използване.

2.7. Ненадзиравани потребителски устройства - потребителите трябва да осигурят оставените без надзор устройства да са подходящо защитени. Потребителите трябва да заключват работния екран на компютъра при напускане на работното място и функцията за автоматично заключване трябва да бъде активирана.

2.8. Политика за чисто бюро и чист екран – при напускане на работното помещение всеки служител премахва всички хартиени носители от бюрото си, които съдържат лични данни. Работният екран на компютъра следва да бъде заключен при напускане на работното място.

## **IX. Сигурност на работата**

**1. Защита от злонамерен софтуер** – осигурена е защитата на информацията и средствата за обработване на информация от злонамерен софтуер.

Механизмите за контрол срещу злонамерен софтуер трябва да бъдат прилагани механизми за контрол за откриване, предотвратяване и възстановяване, които да защитят от злонамерен софтуер и които са съчетани с подходящо осведомяване на потребителите. На ключови работни места има инсталиран надежден платен антивирусен софтуер, който да предпазва работното място от злонамерен софтуер и вируси.

**2. Резервиране –защита на информацията от загуба.**

Резервирането на информация трябва да бъдат направени и редовно изпитвани резервни копия на информация, софтуер и образи на системите. Организацията трябва да има система за резервиране, която да прави веднъж седмично архив на всяко едно работно място. Архивът трябва да може да осигурява цялостно възстановяване на работното място включително възстановяване и на операционната система.

**3. Регистриране и наблюдение** – да се записват събития и да се създадат доказателства.

3.1. Регистриране на събития - трябва да бъдат изработвани, съхранявани и редовно извършвани прегледи на регистри за събития, записващи дейности на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията.

3.2. Защита на регистрираната информация - средствата за регистрация и регистрираната информация трябва да бъдат защитени от подправяне и неоторизиран достъп.

3.3. Дневници на действията на системния администратор и оператора - действията на системния администратор и оператора трябва да бъдат регистрирани, като дневниците трябва да бъдат защитени и редовно преглеждани.

3.4. Синхронизация на часовниците - часовниците на всички системи за обработване на информация в организацията или зоната за сигурност трябва да бъдат синхронизирани с един единствен опорен източник на точно време.

**4. Контрол на работещия софтуер** – да се осигури цялостността на работещите системи

Инсталирането на софтуер върху работещи системи трябва да има изградени права, кои потребители имат право да инсталират софтуер върху работните системи. Обикновените потребители следва да нямат права да инсталират и деинсталират софтуер върху работните системи.

**5. Управление на техническата уязвимост** - да се предотврати използването на технически уязвимости.

5.1. Управление на техническите уязвимости - трябва да бъде получена навременна информация за техническа уязвимост на използваните информационни системи; излагането на организацията на такава уязвимост трябва да бъде оценено и трябва да бъдат предприети мерки, за да се отговори на свързания с това риск. Системният администратор трябва да следи за информация за технически уязвимости.

5.2. Ограничения при инсталиране на софтуер – софтуерът трябва да се инсталира единствено и само от служители с пълни администраторски права.

## **X. Сигурност на комуникациите**

1. Управление на сигурността на мрежите – осигурена е защита на информацията в мрежите и поддържащите ги средства за обработване на информация.

1.1. Механизми за контрол на мрежите - мрежите са управлявани и контролирани, за да защитят информацията в системите и приложенията.

1.2. Сигурност на мрежовите ресурси – механизмите за сигурност, нивата на услугата и изискванията за управление на всички мрежови услуги са определени и включени във всяко споразумение за мрежови услуги, независимо от това, дали тези услуги се предоставят от самата организация или от външна организация.

1.3. Разделяне на мрежите - вътре в мрежите групите информационни услуги, потребители и информационни системи трябва да бъдат разделени.

2. Обмен на информация – поддържа се сигурността на информацията, обменена вътре в организацията или с външни страни.

2.1. За обмен на информация - съществуват официални политики, процедури и механизми за контрол, за да се защити обменът на информация чрез използване на всички средства за комуникация.

2.2. Споразумение за обмен на информация - при прехвърляне на информация за дейността между институцията и външни страни се сключват споразумения.

2.3. Електронен обмен на съобщения - информацията, съдържаща се в електронните съобщения, е подходящо защитена. Всички електронни съобщения трябва да се проверяват от антивирусен софтуер. Съобщенията, съдържащи лични данни трябва да бъдат задължително криптирани чрез софтуер за криптиране.

2.4. Споразумение за поверителност или неразкриване на тайна – в институцията са определени, редовно преглеждани и документирани изисквания за споразумения за поверителност или за неразкриване на тайна, отразяващи потребностите на организацията с оглед защита на информацията.

## **XI. Взаимоотношения с доставчици**

1. Сигурност на информацията при взаимоотношения с доставчици – осигурена е защита на активите на институцията, които са достъпни за доставчика.

1.1. Сигурността на информацията при взаимоотношения с доставчици - с доставчика са договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията.

1.2. Разглеждане на сигурността в рамките на споразумения с доставчици - всички приложими изисквания към сигурността на информацията са въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията.

1.3. Верига за доставки на информационни и комуникационни технологии - споразуменията с доставчиците включват изисквания, отнасящи се за рисковете за сигурността на информацията, свързани с веригата за доставки на услуги и продукти на информационни и комуникационни технологии.

2. Управление на предоставянето на услуги от доставчици – поддържа се договореното ниво на сигурност на информацията и предоставянето на услуги в съответствие със споразуменията с доставчици.

2.1. Наблюдение и преглед на услуги, предоставяни от доставчици - редовно се наблюдават, преглеждат и одитират предоставяните услуги от доставчиците.

2.2. Управление на измененията на услугите, предоставяни от доставчици - измененията на предоставянето на услуги от доставчици, съдържащи поддържане и усъвършенстване на съществуващи политики, процедури и механизми за контрол за сигурност на информацията, трябва да бъдат управлявани, като се отчита критичността на

информацията, системите и процесите, свързани с дейността и повторно оценяване на рисковете.

## **ХII. Управление на инциденти със сигурността на информацията**

1. Управление на инциденти и подобряване на сигурността на информацията – осигурен е последователен и ефикасен подход към управление на инцидентите със сигурността на информацията, включително съобщаване за събития и слабости, свързани със сигурността.

1.1. Отговорности и процедури – установени са отговорности и процедури за управление, за да се осигури бърза, ефикасна и системна реакция на инцидентите със сигурността на информацията.

1.2. Докладване за събития свързани със сигурността на информацията – всички събития, свързани със сигурността на информацията, биват докладвани на ръководството на 79. СУ Индира Ганди .

1.3. Докладване за слабости в сигурността на информацията – изисква се от служителите и доставчиците, използващи информационните системи и услуги на организацията, да отбелязват и докладват всяка наблюдавана или предполагаема слабост в сигурността на системите и услугите. Ако бъде констатиран проблем, трябва незабавно да се уведоми Длъжностното лице по защита на данните и/или ръководството на 79. СУ Индира Ганди .

1.4. Оценяване на събития, свързани със сигурността на информацията и вземане на решения за тях – събитията, свързани със сигурността на информацията, трябва да бъдат оценени, като трябва да бъде решено дали те трябва да бъдат класифицирани като инциденти със сигурността.

1.5. Реакция при инциденти на със сигурността на информацията – при наличие на инциденти със сигурността на информацията се реагира в съответствие с документираните процедури.

1.6. Изводи от инцидентите със сигурността на информацията – познанията, придобити при анализирането и разрешаването на инциденти със сигурността на информацията, се използват за намаляване на вероятността или въздействието на бъдещи инциденти.

1.7. Събиране на доказателства – администраторът трябва да определи и прилага софтуер за идентифициране, събиране, придобиване и съхраняване на информация, която може да послужи като доказателство.

## **ХIII. Съответствие**

1. Съответствие със законови и договорни изисквания – цели се пълно съответствие с нормативни или договорни задължения, отнасящи се към сигурността на информацията, както и на всички изисквания за сигурност.

1.1. Защита на записите – записите са защитени от изгубване, изтриване, разрушаване, фалшифициране, неоторизиран достъп или неоторизирано огласяване в съответствие със законовите, нормативните и договорните изисквания и изисквания за дейността.

1.2. Тайна и защита на информацията за самоличността – осигурена е тайната и защита на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.

1.3. Регламентиране на криптографски механизми за контрол – криптографски механизми за контрол и защита трябва да се използва в съответствие с всички приложими споразумения, нормативни актове и регламенти.

#### **XIV. Прегледи на сигурността на информацията**

1. Независим преглед на сигурността на информацията – през планирани интервали или при настъпили съществени промени се извършва независим преглед на подхода на организацията за управление на сигурността на информацията и неговото прилагане.

2. Съответствие с политиката и стандартите за информационна сигурност – Длъжностното лице по защита на личните данни трябва ежегодно да преглежда доколко обработването на информация и процедурите в тяхната област на отговорност съответстват на подходящите политики за информационна сигурност, стандартите и всякакви други изисквания за сигурност.

3. Преглед на техническото съответствие – информационните системи редовно биват прегледани за съответствие с политиките за сигурност на информацията в организацията и стандартите за сигурност.