36. СУ „МАКСИМ ГОРКИ”
гр. София - 1680, р-н Красно село, ул. „Пирински проход“ № 35
тел. 087 960 9570 /канцелария/; 087 963 9377/директор/;
e-mail*:* info-2209036@edu.mon.bg **; www.36 SOU.com**

УТВЪРЖДАВАМ: Х

Директор: Луиза Накова

ВЪТРЕШНИ ПРАВИЛА

ЗА КИБЕРСИГУРНОСТ И ИНФОРМАЦИОННО ОСИГУРЯВАНЕ

Утвърдени със Заповед № РД-12-1844/14.09.2026 г.

1. Цел, обхват и правни основания

1.1 Настоящите вътрешни правила уреждат организацията, мерките и отговорностите за киберсигурност, мрежова и информационна осигуреност, както и защитата на личните данни в 36. СУ „Максим Горки“ /Училището/.

1.2 Правилата се прилагат за всички служители, педагогически специалисти, непедагогически персонал, ученици (в приложимата част), както и за външни изпълнители и посетители, които имат достъп до информационни активи на Училището.

1.3 Правни основания:

- ***Закон за киберсигурност (ЗКС)*** – общи изисквания за организация и контрол на киберсигурността.
- ***Наредба № Н-6 от 21.12.2022 г.*** за минимални и препоръчителни мерки за мрежова и информационна сигурност.
- ***Закон за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679 (GDPR)*** – изисквания за защита на личните данни.
- Други вътрешни актове на Училището (Правилник за дейността, Правилник за вътрешния трудов ред, Етичен кодекс на училищната общност и др.)

2. Термини и дефиниции (съгласувани с ЗКС, Наредба № Н-6 и GDPR)

- **Информационен актив** – данни, информационни системи, приложения, мрежово и крайно оборудване, носители, хартиени архиви, конфигурации и документация.
- **Инцидент в киберсигурността** – събитие, което компрометира или застрашава поверителността, целостта или наличността на информационните активи.
- **Лични данни** – всяка информация, отнасяща се до идентифицирано или идентифицируемо физическо лице.
- **Обработващ лични данни (външен изпълнител/поддържаща фирма)** – лице, което обработва лични данни от името на администратора (Училището).
- **Администратор** – Училището в качеството му на администратор на лични данни.

3. Роли и отговорности (минимален модел)

3.1. **Директор** – утвърждава правилата; организира и контролира изпълнението им; осигурява ресурси; сключва договори и DPA с външни изпълнители.

3.1.1. За избягване на съмнения: директорът **не носи лична имуществена отговорност** за вреди, причинени от виновни действия/ бездействия на служители или външни изпълнители, извършени в противоречие с писмените му указания и извън предоставените правомощия. Отговорността се носи от нарушителя и/ или от юридическото лице по реда на закона.

3.2. **Координатор по киберсигурност и информационна безопасност** – Мирослава Хаджиева, ръководител направление ИКТ, изпълнява функциите по оперативно прилагане на правилата; управление на риска, контрол на достъпите, логовете, бекъпите, приемане и регистриране на инциденти, поддържане на регистри (раздел 4), комуникация с поддържащата фирма.

3.2.1. При възникване на необходимост, Координаторът може да възлага технически задачи на поддържащата фирма само чрез тикет/писмено задание.

3.3. **Длъжностно лице по защита на данните (DPO) –** Елена Златева, адвокат.

3.3.1. Задачи по чл. 39 GDPR:

(а) информира и консултира администратора и служителите относно задълженията им по GDPR/ЗЗЛД;
(б) наблюдава спазването на изискванията и политиките, включително разпределяне на отговорност, повишаване на осведомеността и обучение;
(в) консултира относно DPIAи следи за нейното изпълнение по чл. 39 GDPR;
(г) сътрудничи на КЗЛД и действа като контактна точка;
(д) отговаря на запитвания на субекти на данни.
3.3.2. DPO действа **независимо,** докладва пряко на Директора и не получава указания относно изпълнението на задачите си. (чл. 39 GDPR).
3.4. **Служители и педагогически специалисти** – спазват правилата; докладват незабавно инциденти/подозрителни събития; преминават обучения.
3.5. **Ученици** – използват училищните системи само за учебни цели; спазват правилата за приемливо ползване; докладват нередности.
3.6. **Външна поддържаща фирма (Обработващ)** – изпълнява договор и DPA; прилага мерките по раздел 7 и 12; носи договорна отговорност.

4. Класификация на активите и регистри
4.1. Води се **Регистър на обработванията на лични данни** по чл. 30 GDPR.
4.2 Води се **Регистър на инцидентите.**

5. Управление на риска и планиране
5.1. Координатора, съвместно с DPO и външната поддържаща фирма ежегодно провеждат оценка на риска за основните системи и услуги; резултатите се документират и одобряват от Директора.
5.2. На база оценката се изготвя годишен **План за киберсигурност** и **План за обучение и осведоменост.**
5.3. Извършва се DPIA (оценка на въздействието) при въвеждане на нови технологии/услуги, които вероятно водят до висок риск за правата и свободите (чл. 35 GDPR).

6. Контрол на достъп и идентичност
6.1. Принцип на „минимални права“ и „need-to-know”.
6.2. Уникални потребителски идентификатори; споделени акаунти не се допускат (с изключение на строго контролирани учебни профили без достъп до лични данни).
6.3. Задължителна силна парола и периодична смяна; активиране на **многофакторна идентификация (MFA)** администраторски/отдалечени/ клауд достъпи.

7. Технически и организационни мерки (съобразени с Наредба № Н-6) и информационна безопасност
7.1. **Управление на уязвимости и актуализации:** поддържане на базови конфигурации; редовно обновяване на ОС/приложения/фърмуер; вътрешни срокове за отстраняване – критични до 72 часа, високи до 14 дни, средни до 30 дни.
7.2. **Защита на крайни устройства:** антивирус/антималуер и EDR на всички устройства; забрана за деактивиране от потребител; автоматично заключване на екрана ≤ 10 мин.
7.3. **Резервни копия:** ежедневни инкрементални и седмични пълни копия за критични системи; поне една **offline/immutable** копия; ежемесечни тестове за възстановяване; описани RPO/RTO.
7.4. **Шифроване:** криптиране на мобилни устройства и преносими носители; криптиран пренос (TLS) за поща/файлообмен/услуги; забрана за локално съхранение на ЛД без шифроване и одобрение.
7.5. **Логване и мониторинг:** включени системни/приложни логове; централно съхранение; синхронизация на време (NTP); анализ от Координатора; **минимален срок на съхранение 6 месеца** за критични системи (освен ако закон изисква друго).
7.6. **Мрежова сигурност:** сегментация (административна, учителска, ученическа, гост); админ интерфейси – достъп само от админ сегмент; забрана за публично достъпни админ портове.
7.7. **Контрол на носители и печат:** забрана на нерегламентирани USB; защитен печат за поверителни документи.

7.8. **Физическа сигурност и КЛЮЧОВЕ:** всички ключове за сървърни/комуникационни помещения и шкафове се събират и съхраняват от зам. директор в запечатана кутия/сейф; издават се само срещу подпис и основание; незабавно докладване при загуба.
7.9. **Облачни услуги**: използват се само одобрени платформи; договорно уреждане на мерките и местонахождението на данните; спазване на GDPR при трансфери извън ЕИП.
7.10. **Домашни устройства:** достъп до защитени механизми; разделяне на служебни данни; забрана за локално съхранение на ЛД без шифроване и одобрение.
7.11. **Електронна поща и домейн защити:** задължително SPF, DKIM и DMARC; защита от фишинг и злонамерени прикачени файлове; етикетиране на външни писма.
7.12. **Wi-Fi:** отделни SSID/VLAN за ученици/гости/учители/администрация; силни пароли; периодична ротация; забрана за WPS; достъп до администраторски устройства само по списък.
7.13. **Привилегирован достъп:** отделни администраторски акаунти.
7.14. **Управление на промени:** промени по системи/ мрежа само след одобрение; план за връщане.
7.15. **Видеонаблюдение (ако е приложимо):** уникални администраторски пароли; ограничен достъп; криптиран достъп; документация на сроковете за съхранение и целите; забрана за неоторизирано облачно споделяне на записи; достъп само на оправомощени лица.

8. Защита на личните данни (GDPR/ЗЗЛД)
8.1. Училището като **администратор** обработва лични данни законосъобразно, добросъвестно и прозрачно, спазва принципите по чл. 5 GDPR.
8.2. **DPO**: Елена Златева – длъжностно лице по защита на данните по чл. 37 GDPR.
8.3. Осигуряват се **правата на субектите** (достъп, корекция, изтриване, ограничаване, възражение, преносимост), срокове и процедури за отговор.
8.4. **Споразумения с обработващи** по чл. 28 GDPR – задължителни за всички външни изпълнители (вкл. поддържащата фирма).
8.5. **Нарушения на сигурността на личните данни:** процедури за откриване, докладване вътрешно до Координатора и DPO; оценка на риска; уведомяване на **КЗЛД** в 72 часа (чл. 33 GDPR) и на засегнатите лица при по-висок риск (чл. 34 GDPR).

9. Обучение и осведоменост
9.1. задължително въвеждащо обучение на новоназначени и ежегодно опреснително обучение за всички служители; тематични кампании за ученици, цифрова хигиена, онлайн безопасност).
9.2. документиране на участията; тестове и симулации (напр. фишинг) по преценка на координатора.

10. Управление на промени и внедряване
10.1. Нови системи/услуги се въвеждат след одобрение от директора по мотивирано предложение от Координатора, включващо оценка на риска и, при необходимост, DPIA.
10.2. Провеждат се тестове в контролирана среда; поддържа се документация и план за обратно връщане.

11. Управление на инциденти и непрекъсваемост
11.1. **Откриване и докладване:** всеки служител/ученик незабавно уведомява **Координатора** (зам. директор) и контактното лице от поддържащата фирма.
11.2. **Класификация:** нисък/среден/висок/критичен; при засягане на лични данни – уведомяване на назначен/външен DPO при първа възможност.
11.3. **Първоначална реакция:** изолиране на засегнати активи; запазване на доказателства (образи/логове); временно ограничаване на услугата при необходимост.
11.4. **Анализ и възстановяване:** определяне на първопричина; корективни действия; възстановяване на резервни копия; верификация.
11.5. **Нарушения на лични данни:** вътрешна оценка на риска; подготовка и уведомяване на **КЗЛД в 72 часа** (чл. 33 GDPR) и до субектите при висок риск (чл. 34 GDPR).
11.6. **Комуникация:** координирана вътрешна и външна комуникация от Директора/упълномощено лице; забрана за самоволно разгласяване.

11.7. **Регистър на инцидентите:** уникален номер; дата/час; система; описание; засегнати лични данни; мерки; уведомявания; отговорни лица; статус.

12. Външна поддържаща фирма – договорни изисквания и отговорност

12.1**.** Всяка услуга по поддръжка/хостинг/облачни услуги/ИТ консултации се възлага с писмен договор и Приложение „Обработване на лични данни“ (DPA) по чл. 28 GDPR.

12.2. **Статут по GDPR:** поддържащата фирма действа по чл. 4, т.8 и чл. 28 GDPR. Не се изисква регистрация като „администратор на лични данни“ пред КЗЛД; този режим е отменен след влизане в сила на GDPR. Ако фирмата обработва лични данни за собствени независими цели, тя е самостоятелен администратор за тези цели, отделно от обработването за Училището.

12.3. **Конфиденциалност:** всички техници на изпълнителя подписват декларация за конфиденциалност и съхранение на лични данни преди допуск до системи/помещения.

12.4. **Достъп и проследимост:** персонализирани временни акаунти; достъп само след тикет/писмено разрешение; дейностите се логват; задължително заключване на шкафове/помещения след работа.

12.5. **Инциденти:** изпълнителят съобщава без неоправдано забавяне за всяко нарушение на сигурността; съдейства при уведомявания/разследване/възстановяване.

12.6. **Отговорност:** при хардуерно/физическо компрометиране или друг инцидент, настъпил поради немарливост на изпълнителя или оставени „вратички“ (незаключени шкафове, default пароли, неизтрити тестови акаунти, публични админ портове, деактивирани защити без одобрение), изпълнителят носи договорна отговорност, включително неустойки и обезщетения за преки вреди съгласно договора/DPA.

12.7. **Приключване на услугата:** след прекратяване на услугата изпълнителят връща/изтрива данните и предоставя декларация за изпълнение; предава всички ключове/достъпи; унищожава конфиденциални копия.

13. Приемливо ползване и поведение

13.1. Забранено е инсталирането на неоторизиран софтуер и свързване на непозволени устройства към мрежата.

13.2. Служебният e-mail и облачните ресурси се използват за служебни цели; забранено е препращане на списъци с лични данни към лични пощи.

13.3 Публикуване на снимки/видео с ученици се извършва само при налично правно основание и информирано съгласие GDPR/ЗЗЛД и вътрешни процедури.

14. Документация, отчетност и одит

14.1. Поддържат се актуални: регистри по Раздел 4, политики (пароли, бекъп, клауд), инструкции и планове (BC/DR, инциденти).

14.2. Координаторът и DPO изготвят годишен **Отчет за състоянието на киберсигурността и защитата на личните данни**, представян на Директора до 31 декември.

14.3. планират се вътрешни проверки и, при необходимост, външни одити.

15. Нарушения и дисциплинарни мерки и отговорности

15.1. Нарушенията на настоящите правила подлежат на дисциплинарна отговорност по Кодекса на труда и вътрешните актове, както и на търсене на имуществена отговорност при вреди.

15.2. При нарушения на личните данни се прилагат процедурите по раздел 8 и 11 и се уведомяват компетентните органи.

15.3. **Отговорност на служители:** при изтичане на информация или кибератака, причинени от виновно действие /бездействие на служител (напр. споделяне на парола, инсталация на неоторизиран софтуер, заобикаляне на мерки, неприлагане на указания), съответния служител носи дисциплинарна и имуществена отговорност по КТ.

15.4. **Отговорност на поддържащата фирма:** при физическо/хардуерно компрометиране или друг инцидент, настъпил поради немарливост/вратички от страна на изпълнителя(по т.12.7), се търси договорна отговорност -неустойки/обезщетение; Училището си запазва правото да търси по-големи вреди по общия ред.

15.5. Роля на директора: директорът организира и контролира изпълнението на правилата, но не носи лична имуществена отговорност при липса на вина и при добросъвестно изпълнение на нормативните си задължения; отговорността се носи от нарушителя и/или от юридическото лице по реда на закона.

16. Влизане в сила и актуализация

16.1. Правилата влизат в сила от датата на заповедта по-горе.

16.2. Преглеждат се най-малко веднъж годишно и при осъществени промени в рисковете, технологиите или правните изисквания.

17. Преходни и заключителни разпоредби

17.1. В **5-дневен срок** от влизане в сила на правилата всички ключове за сървърни/комуникационни помещения и шкафове се предават на Мирослава Хаджиева, ръководител направление ИКТ**.**

17.2. В 10-дневен срок се създава и започва водене на **Регистър на инцидентите.**

17.3. В 30-дневен срок се сключва /актуализира **DPA** с поддържащата фирма по чл. 28 GDPR и се събират декларации за конфиденциалност.

17.4. DPIA се извършва **при наличие на предпоставки** по чл. 35 GDPR; при липса на DPIA за планирана високорискова дейност внедряването **се отлага** до приключването ѝ.

Приложение А – Задължителни клаузи към договор с поддържащата фирма (DPA) (шаблон)

1. Предмет: обработване на ЛД за целите на ИТ поддръжка/администрация на системи на училището.
2. Категории данни/субекти: служители, ученици, родители/настойници; идентификационни и академични данни, служебни контакти.
3. Продължителност и място на обработване.
4. Инструкции на администратора; забрана за други цели.
5. Поверителност на персонала на изпълнителя.
6. Мерки за сигурност (описани в Приложение към DPA).
7. Подизпълнители – предварително писмено одобрение.
8. Асистиране при искания на субекти и при инциденти.
9. Уведомяване за нарушение без неоправдано забавяне.
10. Връщане/изтриване на данните след прекратяване.
11. Отговорност: неустойки/обезщетение при виновно неизпълнение; препоръчителна застраховка.

Приложение Б – Декларация за конфиденциалност (техник на изпълнителя) (шаблон)

ДЕКЛАРАЦИЯ
за конфиденциалност от техник на изпълнителя

Аз, долуподписаният, ...,
(трите имена)
служител на ……,
декларирам, че:

1. ще пазя в тайна и няма да разгласявам лични данни и друга защитена информация, до която получавам достъп при поддръжка на системите на 36. СРЕДНО УЧИЛИЩЕ „МАКСИМ ГОРКИ“;
2. ще използвам информацията единствено за целите на изпълнението на задачите по договора;
3. ще спазвам политиките за сигурност на Училището и указанията на упълномощените лица;
4. при инцидент или съмнение ще уведомя незабавно Координатора и контактното лице по договора;
5. при прекратяване на участието ми ще върна всички носители/достъпи и ще унищожа копия.

Дата: …….. /Подпис:…… / ЛН…… / Документ за самоличност …….

Приложение В – Декларация на служителя

ДЕКЛАРАЦИЯ

за запознаване и спазване на Правила за мрежова и информационна сигурност и допустимо използване на активи на 36. СУ „Максим Горки“ – гр. София

Аз,.....
(трите имена)

потвърждавам, че съм прочел(а) и разбрал(а) Правилата за мрежова и информационна сигурност на 36. СУ „Максим Горки“ – гр. София.
Съгласен(на) съм да спазвам изискванията за достъп и употреба на ресурси.
Тази декларация е валидна за периода на моите трудови правоотношения с 36. СУ „Максим Горки“ – гр. София, или до актуализирането на правилата.

Подпис:_____

Длъжност: _____

Дата: _____

Приложение Г – Формуляр за докладване на инцидент (образец)

ФОРМУЛЯР ЗА ДОКЛАДВАНЕ НА ИНЦИДЕНТ

- Дата и час на откриване: …….
- Открит от (име /длъжност /клас): ……..
- Засегната система/устройство: ……
- Описание на събитието: ……
- Вероятно засягане на лични данни: ДА/НЕ (описание):
- Първоначални действия: ……..
- Кой е уведомен: Координатор/Директор/Изпълнител
- Подпис на подателя: ……
- Номер в Регистъра на инцидентите: ……

Забележка: Настоящите правила са съобразени с изискванията на ЗКС, Наредба № Н-6 и ЗЗЛД/GDPR и се допълват от вътрешни политики (Пароли, Бекъп, Облак, Инциденти), утвърждавани от Директора. При противоречие предимство имат приложимите нормативни актове.