гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www

УТВЪРЖДАВАМ:

ДИРЕКТОР: РАЛИЦА КИРИЛОВА

ВЪТРЕШНИ ПРАВИЛА

ЗА КИБЕРСИГУРНОСТ, МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ И ЗАЩИТА НА ИНФОРМАЦИОННИТЕ АКТИВИ

В 18. СУ „УИЛЯМ ГЛАДСТОН“

Приети с Протокол № РД-04-17/11.09.2026 г. на Педагогически съвет и влизат в сила от 15.09.2026 г.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите правила уреждат организацията, отговорностите и основните организационни и технически мерки за киберсигурност, мрежова и информационна сигурност, защита на информационните активи, управление на достъпа, инцидентите, непрекъсваемостта и рисковете, свързани с външни ИКТ доставчици.

(2) Целта е осигуряване на подходящо ниво на защита, съобразено с характера на дейността, използваните системи, наличните ресурси и установените рискове.

Чл. 2. Правилата се прилагат от директора, заместник-директорите, педагогическите специалисти, административния и помощния персонал, учениците в приложимата част, както и за външни изпълнители и други лица с предоставен достъп до информационни ресурси на Училището.

II. НОРМАТИВНА УРЕДБА

Чл. 3. Правилата се прилагат в съответствие със:

1. Закона за киберсигурност;

2. приложимите подзаконови нормативни актове, издадени на основание Закона за киберсигурност, включително Наредбата за минималните изисквания за мрежова и информационна сигурност;

3. Регламент (ЕС) 2016/679 (GDPR);

4. Закона за защита на личните данни;

5. приложимите нормативни актове в областта на предучилищното и училищното образование;

6. вътрешните актове на 18. СУ „Уилям Гладстон“.

Чл. 4. Мерките се прилагат съобразно приложимите към Училището нормативни изисквания и пропорционално на установения риск, характера на информационните активи и възможните последици от инцидент.

III. ОСНОВНИ ПОНЯТИЯ

Чл. 5. По смисъла на настоящите правила:

1. „Информационен актив“ е информация, информационна система, база данни, приложение, мрежово или крайно устройство, технически носител, конфигурация, документ или друг ресурс със стойност за дейността.

2. „Киберинцидент“ е събитие, което засяга или може да засегне наличността, автентичността, цялостността или поверителността на данни, мрежи, системи или услуги.

3. „Нарушение на сигурността на личните данни“ се разбира по смисъла на Регламент (ЕС) 2016/679.

4. „Привилегирован достъп“ е право за администриране, конфигуриране или управление на система, мрежа или ресурс.

5. „Външен изпълнител“ е лице, което предоставя ИКТ, технически, облачни, хостинг или други свързани услуги.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

IV. ОРГАНИЗАЦИЯ, РОЛИ И ОТГОВОРНОСТИ

Чл. 6. (1) Директорът организира и контролира изпълнението на правилата, утвърждава вътрешни процедури, осигурява ресурси в рамките на възможностите, определя длъжностни лица, одобрява съществени промени в инфраструктурата, организира действията при значим инцидент и осигурява обучение.

(2) Отговорността при нарушение се определя съгласно действащото законодателство и конкретните факти.

Чл. 7. (1) Директорът определя със заповед координатор по информационна и киберсигурност.

(2) Координаторът подпомага директора; координира идентифицирането на активите и оценката на риска; следи управлението на потребителските права и привилегирования достъп; координира дейностите по резервно копиране и възстановяване на данни; приема и регистрира сигнали за киберинциденти; координира работата с външни ИКТ изпълнители; поддържа регистъра на инцидентите и информира директора при съществен риск или инцидент.

Чл. 8. (1) Длъжностното лице по защита на данните (DPO) изпълнява функциите по чл. 37-39 от Регламент (ЕС) 2016/679.

(2) DPO информира и консултира, наблюдава спазването на правилата за защита на данните, предоставя становища относно оценки на въздействието и сътрудничи с КЗЛД.

(3) DPO действа независимо и при организация, която не допуска конфликт на интереси.

Чл. 9. Оперативното вземане на технически решения по киберсигурността и контролните функции на DPO се разграничават организационно.

Чл. 10. Всеки служител е длъжен да спазва правилата, да използва ресурсите по предназначение, да пази идентификаторите си, да не предоставя пароли, да докладва незабавно съмнения за инцидент и да участва в определените обучения.

Чл. 11. Учениците използват училищните информационни ресурси за образователни цели и при условията на Правилника за дейността на Училището и правилата за приемливо използване.

V. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ И РИСКА

Чл. 12. Училището поддържа актуална информация за основните информационни активи: сървъри, мрежово оборудване, работни станции, мобилни устройства, системи и приложения, бази данни, облачни услуги, домейни, електронна поща, видеонаблюдение, резервни копия и външни услуги с достъп до ресурси.

Чл. 13. За информационните активи се определя необходимо ниво на защита според тяхната критичност, вида на информацията и последствията при загуба, изменение, унищожаване или неправомерен достъп.

Чл. 14. (1) Периодично и при значителна промяна на системите се извършва оценка на риска.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

(2) Отчитат се заплахите, уязвимостите, вероятността, последиците за дейността и физическите лица и зависимостта от външни доставчици.

(3) Оценката се документира и при необходимост се изготвя план за намаляване на риска.

VI. УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТИ И ДОСТЪП

Чл. 15. Достъпът се предоставя според принципите „необходимост да се знае“, минимално необходимите права, индивидуална отчетност и разделение на функциите, когато е приложимо.

Чл. 16. Всеки потребител използва индивидуален профил, когато е технически възможно. Споделени административни профили се избягват и при неизбежност се контролират и проследяват.

Чл. 17. Използват се силни пароли, които отговарят на утвърдените вътрешни изисквания за дължина, сложност и защита**.** Те се променят при първоначално предоставяне, съмнение или установено компрометиране и в други случаи, определени въз основа на риска.

Чл. 18. Многофакторна автентикация се активира за администраторски, отдалечени и облачни достъпи, когато системата предоставя такава техническа възможност.

Чл. 19. При прекратяване на трудово, договорно или друго правоотношение достъпите се прекратяват своевременно; при промяна на функцията предоставените права се преразглеждат.

VII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл. 20. Съобразно риска и техническите възможности се прилагат мерки за защита от зловреден софтуер, актуализации, крайни устройства, уязвимости, мрежова защита и сегментация, резервно копиране, криптиране, логване и наблюдение, физическа защита, управление на промени и привилегирован достъп.

Чл. 21. Системите и приложенията се поддържат с актуални и поддържани версии, доколкото това е технически и организационно възможно. Уязвимостите се оценяват според риска и се предприемат своевременни мерки за отстраняване или ограничаване. Вътрешни целеви срокове могат да се определят с отделна техническа процедура.

Чл. 22. Крайните устройства се защитават с приложими средства срещу зловреден софтуер, конфигурират се за автоматично заключване след подходящ период на неактивност и не трябва да позволяват на обикновени потребители да деактивират основни механизми за защита.

VIII. РЕЗЕРВНИ КОПИЯ И ВЪЗСТАНОВЯВАНЕ

Чл. 23. За критичните данни и системи се организира резервно копиране с честота, определена въз основа на риска, характера и променливостта на информацията.

Чл. 24. Когато е технически възможно, се поддържа отделено резервно копие, достъпът се ограничава, периодично се тества възстановяването и се определят целеви параметри за допустима загуба на данни и време за възстановяване.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

IX. МРЕЖОВА И БЕЗЖИЧНА СИГУРНОСТ

Чл. 25. Училищната мрежа се организира, доколкото е приложимо, с логическо разделение между административни ресурси, ресурси за обучение и ученици, гостов достъп и критични ресурси.

Чл. 26. Административните интерфейси на мрежово и системно оборудване се ограничават до оправомощени потребители и защитени сегменти.

Чл. 27. Безжичните мрежи се защитават със съвременни механизми за автентикация и криптиране; не се използват остарели или компрометирани методи за защита.

X. ЕЛЕКТРОННА ПОЩА, ОБЛАЧНИ УСЛУГИ И МОБИЛНИ УСТРОЙСТВА

Чл. 28. Служебната електронна поща се използва преимуществено за служебни цели. Не се изпращат служебна информация и лични данни към лични електронни пощи без обоснована необходимост, правно основание и подходяща защита.

Чл. 29. При управление на домейни и електронна поща се прилагат подходящи механизми за защита от подправяне на изпращача, фишинг и злонамерено съдържание, включително SPF, DKIM и DMARC, когато са технически приложими.

Чл. 30. Облачни услуги се използват след оценка на сигурността, условията за обработване на данни, правата за достъп, местонахождението и трансферите на данни, когато е приложимо, както и възможностите за извличане и заличаване при прекратяване.

XI. ФИЗИЧЕСКА СИГУРНОСТ

Чл. 31. Достъпът до помещения и шкафове с критично мрежово, сървърно и комуникационно оборудване се ограничава до определени лица.

Чл. 32. Ключовете и другите физически средства за достъп се съхраняват контролирано, а предоставянето им се документира, когато характерът на достъпа го изисква. Загуба се докладва незабавно.

XII. ВЪНШНИ ДОСТАВЧИЦИ И ИЗПЪЛНИТЕЛИ

Чл. 33. Достъп на външни изпълнители се предоставя само в необходимия за изпълнение на договора обем.

Чл. 34. Договорите с ИКТ изпълнители включват според предмета им изисквания за поверителност, контрол на достъпа, уведомяване при инциденти, технически и организационни мерки, подизпълнители, връщане или заличаване на информацията, съдействие при проверки и договорна отговорност.

Чл. 35. Когато външен изпълнител обработва лични данни от името на Училището, отношенията се уреждат с договор или друг правен акт по чл. 28 от Регламент (ЕС) 2016/679. Статутът на изпълнителя се определя според реалните му функции и обработването, което извършва.

XIII. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 36. Училището обработва лични данни при спазване на принципите по чл. 5 от Регламент (ЕС) 2016/679.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

Чл. 37. Поддържа се Регистър на дейностите по обработване съобразно чл. 30 от Регламент (ЕС) 2016/679.

Чл. 38. При планиране на обработване, което е вероятно да породи висок риск за правата и свободите на физическите лица, се извършва оценка на въздействието по чл. 35 от Регламент (ЕС) 2016/679.

Чл. 39. При публикуване на снимки, видеозаписи, ученически материали или друга информация с лични данни се осигуряват приложимото правно основание, прозрачност и защита на правата на субектите.

XIV. УПРАВЛЕНИЕ НА КИБЕРИНЦИДЕНТИ

Чл. 40. Всеки служител уведомява незабавно координатора или директора при установен или предполагаем неоторизиран достъп, зловреден софтуер, фишинг, компрометиран профил, загубено устройство, необичайно поведение на система, загуба или повреждане на информация или друга киберзаплаха.

Чл. 41. За инцидента се създава запис **в Регистъра на инцидентите**, съдържащ най-малко дата и час, начин на откриване, засегнати активи, описание, първоначални действия, възможно засягане на лични данни, последващи мерки и статус.

Чл. 42. Според характера на инцидента се предприемат действия за ограничаване, съхраняване на необходимата информация за установяване на причините, отстраняване, възстановяване, анализ и корективни мерки.

Чл. 43. Когато за Училището е приложимо конкретно задължение за уведомяване по Закона за киберсигурност, компетентните органи се уведомяват по реда и в сроковете, установени в закона.

XV. НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 44. При съмнение за нарушение на сигурността на личните данни координаторът уведомява без неоправдано забавяне директора и DPO.

Чл. 45. Извършва се оценка на вида и обема на данните, категориите засегнати лица, вероятните последици, риска за правата и свободите и предприетите ограничителни мерки.

Чл. 46. Когато са налице предпоставките на чл. 33 от Регламент (ЕС) 2016/679, КЗЛД се уведомява без ненужно забавяне и, когато е възможно, не по-късно от 72 часа след узнаването за нарушението.

Чл. 47. Когато нарушението може да породи висок риск за правата и свободите на физическите лица, засегнатите субекти се уведомяват при условията на чл. 34 от Регламент (ЕС) 2016/679.

XVI. ОБУЧЕНИЕ, ОСВЕДОМЕНОСТ И ПРИЕМЛИВО ИЗПОЛЗВАНЕ

Чл. 48. За служителите се организират първоначален инструктаж, периодично обучение, информация за актуални заплахи, обучение за разпознаване на фишинг и за работа с лични данни и служебна информация.

Чл. 49. За учениците се организират подходящи дейности за цифрова грамотност, безопасно поведение онлайн и защита на личната информация.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

Чл. 50. Не се допуска инсталиране на неразрешен софтуер, заобикаляне или деактивиране на защити, споделяне на пароли, използване на чужд акаунт, включване на неразрешени устройства към защитени сегменти, неправомерно копиране или разпространяване на служебна информация и използване на ресурсите за незаконни дейности.

Чл. 51. При използване на лични устройства за служебни цели се предприемат подходящи мерки за разделяне и защита на служебната информация.

XVII. ДОКУМЕНТАЦИЯ, КОНТРОЛ И ПРЕГЛЕД

Чл. 52. Съобразно приложимостта се поддържат регистър на информационните активи, регистър на инцидентите, регистър на дейностите по обработване, оценка на риска, документация за административен достъп, резервно копиране и възстановяване, външни доставчици.

Чл. 53. Правилата и свързаните мерки се преглеждат най-малко веднъж годишно, след значим инцидент, при съществена промяна на инфраструктурата или приложимото законодателство и при установени съществени слабости.

XVIII. ОТГОВОРНОСТ ПРИ НАРУШЕНИЯ

Чл. 54. Служителите носят отговорност за виновно неизпълнение съобразно Кодекса на труда, приложимото законодателство и вътрешните актове на Училището.

Чл. 55. При нарушения от ученици се прилагат ЗПУО, Правилникът за дейността на 18. СУ „Уилям Гладстон“ и другите приложими училищни правила.

Чл. 56. Отговорността на външните изпълнители се определя съгласно договора, приложимото законодателство и конкретните обстоятелства. Наличието на външен доставчик не освобождава Училището от задължения, които законът възлага непосредствено на него.

XIX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Правилата се прилагат съвместно с останалите вътрешни актове на 18. СУ „Уилям Гладстон“.

§ 2. При противоречие между настоящите правила и действащ нормативен акт се прилага нормативният акт.

§ 3. Директорът може да утвърждава отделни инструкции и процедури за техническото изпълнение на правилата.

§ 4. Служителите се запознават с правилата по установения в Училището ред, а външните изпълнители с приложимите към тях изисквания преди предоставяне на достъп.

гр. София – 1303, ул. “Пиротска” № 68, тел.02/988 03 01; 2204018@edu.mon.bg; info@18su.bg www.18su.bg

ПРИЛОЖЕНИЕ № 1

ФОРМУЛЯР ЗА ДОКЛАДВАНЕ НА ИНЦИДЕНТ

Дата и час на установяване: .....

Лице, установило инцидента: .....

Длъжност/клас: .....

Засегната система/устройство: .....

Описание на събитието: .....

Вероятно засягане на лични данни: ДА / НЕ / НЕ Е УСТАНОВЕНО

Предприети първоначални действия: .....

Уведомени: Координатор / Директор / DPO / ИКТ изпълнител / Друго

Номер в Регистъра на инцидентите: .....

ПРИЛОЖЕНИЕ № 2

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ НА ВЪНШЕН ИЗПЪЛНИТЕЛ

Аз, ..., служител/представител на ....., декларирам, че:

1. ще използвам предоставения достъп само за възложените задачи;

2. няма да разкривам лични данни, служебна или друга защитена информация;

3. няма да създавам или запазвам копия извън необходимото за изпълнение на задачата;

4. ще спазвам приложимите правила за информационна и киберсигурност;

5. ще уведомя незабавно при инцидент или съмнение за инцидент;

6. след приключване ще прекратя използването на достъпите и ще върна физическите средства за достъп.

Дата: ..... Име: ..... Подпис: .....

ПРИЛОЖЕНИЕ № 3

КОНТРОЛЕН СПИСЪК ПРИ ПРЕКРАТЯВАНЕ НА ДОСТЪП

☐ Деактивиран служебен акаунт

☐ Деактивирана/променена служебна електронна поща

☐ Премахнати права до облачни платформи

☐ Премахнат VPN/отдалечен достъп

☐ Премахнати административни права

☐ Върнати служебни устройства

☐ Върнати ключове/карти

☐ Променени споделени технически идентификатори, когато е приложимо

☐ Предадени служебни файлове и документация

☐ Отразена промяната в съответната документация