

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“,
с. Старцево, общ. Златоград, обл. Смолян

1. ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Данни за администратора

Администратор	СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян
Адрес	Ул. „П. Яворов“ 4
E-mail	sou_starcevo@abv.bg
Телефон	03073/2084; 0888861762

Раздел I. Цел

1. Настоящият документ предоставя общ преглед на изискванията за защита на данните и насочва към по-подробни указания, ако е необходимо.
2. Въпроси относно политиката могат да бъдат отправяни на e-mail адрес на образователната институция: СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян

Раздел II. Основания

3. Общият регламент за защита на данните (ОРЗД), който е директно приложим в законодателството на България и може да е/е допълнен чрез Закона за защита на личните данни (ЗЗЛД) и други нормативни актове, установява рамка от права и задължения, предназначени да защитават личните данни. В настоящата политика към тях се реферира като "законодателство за защита на данните".
4. Принципите са следните:
 - 4.1. Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин.
 - 4.2. Личните данни, събирани за конкретни, изрично указани и легитимни цели, не се обработват по-нататък по начин, несъвместим с тези цели.
 - 4.3. Личните данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“).
 - 4.4. Личните данни следва да са точни и при необходимост да бъдат поддържани в актуален вид („точност“).
 - 4.5. Личните данни следва да са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни („ограничение на съхранението“).

- 4.6. Прилагат се подходящи технически или организационни мерки срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане („цялостност и поверителност“).
5. ОРЗД задава определени права на субектите на данни, свързани с техните лични данни, които са:
- право на достъп;
 - право на коригиране;
 - право на изтриване (при определени обстоятелства) – правото „да бъдеш забравен“;
 - правото за ограничаване на обработването;
 - право на преносимост (при определени обстоятелства);
 - правото за възражение, включително срещу директен маркетинг;
 - правото да се изисква човешка намеса с оглед на автоматизирани процеси, включително профилиране.
6. Условиата, при които личните данни могат да бъдат прехвърлени в страни извън Европейското икономическо пространство, са определени в ОРЗД. Те включват адекватност, подходящи гаранции, обвързващи корпоративни договори и изрично съгласие, наред с другите.
7. Дефиниране на „лични данни“ и „специални категории лични данни“ (чувствителни данни), съгласно ОРЗД:
- 7.1. „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;
- 7.2. „специални категории лични данни“ са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;
8. Всяка обработка на лични данни следва да почива на поне едно законово основание, съгласно ОРЗД. Възможните основания са (чл. 6 от ОРЗД): договор, законово задължение, жизненоважни интерес, обществен интерес, легитимен интерес и съгласие. Данните за специалните категории изискват по-специално законово

основание (чл. 9 от ОРЗД). Тази законова основа се посочва в Регистър на дейностите по обработването. Служител, който не е сигурен какво правно основание се отнася до личните данни, които възнамерява да обработва, трябва да потърси съвет от Длъжностното лице по защита на личните данни.

Раздел III. Политика и насоки

9. СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян се ангажира с политика за защита на правата и свободите на лицата по отношение на обработката на техните лични данни.
10. Настоящата Политика и допълнителните насоки към нея, се отнасят за всички лични данни, обработвани за целите на институцията, независимо от това къде и как се съхраняват.

Раздел IV. Приложение на политиката

11. СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян обработва лична информация за служители, ученици, родители, и други, определени като субекти на данни в законодателството за защита на данните. Тези данни трябва да се обработват само в съответствие със законодателството за защита на данните, което е и цел на настоящата политика.
12. Всяко нарушение на тази Политика може да доведе до това институцията като администратор на данни (и в някои случаи физическите лица, работещи за нея) да наруши законодателството за защита на данните и да носи отговорност за последиците от такова нарушение.
13. Ръководителите в институцията отговарят за това тя да спазва законодателството за защита на данните. Всички служители трябва да са прочели и разбрали тази политика преди да имат достъп до лични на данни, обработвани от институцията.
14. Отговорност на всички ползватели на лични данни в институцията е да гарантира сигурността на личните данни. Личните данни не трябва да се разкриват на никое неупълномощено лице под каквато и да е форма, случайно или по друг начин.
15. Всяко нарушение или неспазване на настоящата Политика, особено всяко преднамерено разкриване на лични данни на неупълномощена страна, може да доведе до дисциплинарни или други подходящи действия.
16. Институцията периодично проверява спазването на законодателството за защита на данните и политиката и при необходимост актуализира своите насоки в тази област.
17. Всеки неоторизиран достъп до или разкриване на лични данни или други нарушения на сигурността на данните трябва да бъде докладван съгласно Инструкцията за действие при пробив в сигурността на личните данни веднага след установяването им или при наличието на основателно подозрение за настъпило нарушение.
18. Ръководителят ИКТ отговаря за това всички служители в институцията да бъдат информирани за задълженията си съгласно законодателството за защита на данните, включително тяхното обучение и инструктаж.

19. Съвети и подкрепа във връзка със законодателството за защита на данните се предоставят от определения служител за защита на личните данни (СЗД) или назначеното длъжностно лице за защита на личните данни (ДЗЛД).
20. ДЗЛД докладва на ръководството на институцията (*директор*).

Раздел V. Достъп до данни

21. Правото на достъп от страна на субектите на данни следва да се реализира в определен срок от 30 дни. Поради това от съществено значение е предоставяне на исканията за достъп до данни към СЗД/ДЛЗД във възможно най-кратък срок след тяхното получаване, независимо от това, по какъв начин точно е постъпило искането в институцията и до кого е било подадено.

Раздел VI. Съхраняване на данни

22. Личните данни се съхраняват само за времето, необходимо за извършване на обработката, за която са събрани. Това важи както за електронни, така и за не електронни лични данни. Това се разпростира също така и върху резервните копия и копията, направени на преносими носители.

Раздел VII. Трансфер на данни

23. Всеки трансфер на данни, включително използването на облачни услуги, извън ЕИП следва да бъде предварително съгласуван със СЗД/ДЛЗД с оглед изискването в ОРЗД за предприемането на определени мерки.

Раздел VIII. Регистър на дейностите по обработването

24. Регистърът на дейностите по обработването се използва, за да се отговори на изискванията за съхранение на данни в законодателството за защита на данните (Приложение I).
25. Отговарящите за отделните организационни и оперативни дейности, които формират целите на обработваната информация, осигурят създаването и поддържането на **актуалността на информацията в регистъра**.
26. Всяка година те извършват преглед на актуалността.
27. ДЗЛД гарантира, че притежателите на информационни активи получават подходяща помощ за поддържане на регистъра.

Раздел IX. Технически и организационни мерки за защита на данните

28. Институцията въвежда подходящи технически и организационни мерки (ТОМ), за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с ОРЗД, като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица.
29. Техническите и организационните мерки следва да допринесат за защита на данните на етапа на проектирането и по подразбиране. Същите са посочени в Инструкция за техническите и организационни мерки на институцията във връзка с обработването на лични данни.

30. В техническите и организационните мерки институцията изрично предвижда минимално необходимите реквизити при сключване на споразумения с обработващи данни, така че да се постигне ниво на защита не по-ниско от прилаганото от самата институция.

Раздел X. Съответствие, свеждане до знание и дисциплинарни процедури

31. Нарушаването на поверителността на личните данни е и нарушение на законодателството за защита на данните и може да доведе до наказателен или граждански иск срещу институцията. Следователно всички обработващи лични данни в институцията трябва да се придържат към политиката за защита на личните данни и политиките, които допринасят за нейното изпълнение.
32. Всички настоящи служители и други упълномощени потребители биват информирани за наличието на тази политика и наличието на съпътстващи политики, процедури, инструкции и насоки.
33. Всички служители подписват Декларация за поверителност (Приложение II).
34. Всяко нарушение на сигурността ще бъде разгледано в съответствие с правила на институцията и съответните дисциплинарни политики.

Приложения

№	Наименование на приложението
1	Приложение I: 1. Регистър на дейности по обработване на лични данни (администратор) 2. Регистър на категории дейности по обработването (обобщаващ)
2.	Приложение II 1. Регистър на лицата, обработващи лични данни 2. Списък на лица, които обработват лични данни
3	Приложение II: Декларация за поверителност на данните

**Политика за техническите и организационни мерки
за защита на личните данни**

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС І“,
С. Старцево, общ. Златоград, обл. Смолян

**ПОЛИТИКА ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА**

Въведение

Настоящата политика е разработена въз основа на насоките в Общия регламент за защита на личните данни, съгласно който защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки (ТОМ), за да се гарантира изпълнението на изискванията на Общия регламент за защита на личните данни.

Раздел I. Основни принципи

1. За всяка конкретна обработка институцията осигурява подходящи технически и организационни мерки за защита на личните данни, отчитайки:
 - 1.1. Достиженията на техническия прогрес.
 - 1.2. Разходите за прилагане на мерките.
 - 1.3. Естеството на обработването.
 - 1.4. Обхвата на обработването.
 - 1.5. Контекста и целите на обработването.
 - 1.6. Възможните рискове за правата и свободите на физическите лица.
 - 1.7. Рискове от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.
2. Основен принцип, който институцията спазва, е да не се обработват повече от необходимите лични данни, като това се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.
3. Данните следва да се обработват само от лицата, обработващи тези данни по указание на администратора.
4. Процесът по обработката следва да бъде документиран.

Раздел II. Насоки за изграждане на система от технически и организационни мерки (ТОМ) за защита на личните данни

5. С оглед на важното значение на ТОМ по отношение на налаганите глоби от надзорния орган, институцията следва да реализира мерки, които се основават на:
 - 5.1. обучение на служителите, обработващи лични данни;
 - 5.2. документална обезпеченост на процесите, включително документиране на самите процеси;

Политика за техническите и организационни мерки за защита на личните данни

- 5.3. мониторинг на обработването на данни за своевременно откриване на пробиви в сигурността;
- 5.4. залагане на изискванията на ОРЗД в нормалните дейности на институцията (избор на доставчици, използване на информационни системи и т.н.).

Раздел III. Приложимо ниво на риск

- 6. С оглед на множеството паралелни дейности, които се извършват в институцията, тя възприема единна оценка на риска на всички свои дейности, прилагайки най-високия, установен такъв.
- 7. До наличието на официална национална методология за определяне нивото на риска, институцията приема, че нивото на риск на обработването на данни като администратор се приема за „ниско“ – неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.
- 8. В случай, че институцията е обработващ данни, съответните технически и организационни мерки се определят в договора със съответния администратор или нормативен акт, който регулира това отношение. Институцията си запазва правото самостоятелно да въведе допълнителни мерки за сигурност, които смята за необходими.

Раздел IV. Технически и организационни мерки за защита на личните данни

- 9. Мерките, посочени по-долу, се основават на възприетото ниво на риск в т.7.
- 10. Не всички мерки е възможно да се отнасят към обичайната дейност на институцията, но е възможно необходимостта от тях да възникне при дейността на обработващите за институцията данни от трети страни или такива, които създават специфични решения за нея.
- 11. Техническите и организационни мерки се прилагат, доколкото се поддържа от функционалността на съответното устройство или операционна система, и се използват от институцията във връзка с осъществяването на съответния процес.
- 12. Мерки, насочени към документалното и оперативното изпълнение на мерките за защита на личните данни:
 - 12.1. Налична е политика за защита на личните данни;
 - 12.2. Налична е процедура за действие при нарушение на личните данни;
 - 12.3. Описание на техническите и организационните мерки по отношение на защита на лични данни.
 - 12.4. Субсидиарно се прилагат и:
 - 12.4.1. Политика за информационна сигурност;
 - 12.4.2. План за непрекъсваемост на работните процеси.
- 13. Мерки, насочени към служителите:
 - 13.1. Информирание и засилване на чувствителността на служителите по отношение на обработването на лични данни, включително чрез провеждането на начални обучения;
 - 13.2. Налагане на задължителна инструкция за допустимата употреба на компютърни устройства на институцията включително налагане на дисциплинарни наказания при нейното нарушаване;
 - 13.3. Служителите биват информирани и подписват декларация за поверителност.

**Политика за техническите и организационни мерки
за защита на личните данни**

14. Мерки, насочени към достъпване на информационните системи на институцията.
 - 14.1. Всеки потребител има свой уникален акаунт, който следва да не споделя с никой друг;
 - 14.2. Налице е политика за сложност на паролите за достъп до акаунта, обхващаща всички устройства на институцията (вкл. смартфони, таблети, лаптопи, стационарни компютри, сървъри и т.н.);
 - 14.3. Потребителите следва да променят редовно своята парола, по възможност наложено от самите електронни системи;
 - 14.4. Неуспешните опити за достъп до акаунтите следва да бъде ограничен;
15. Мерки насочени към управление на даването на достъпи до информационните системи на институцията.
 - 15.1. Потребителите имат различни акаунти (профили) за отделните задачи, които извършват;
 - 15.2. Всички ненужни права (например вследствие на напускане или преместване) следва да се премахват своевременно;
 - 15.3. Всички стари права подлежат на редовен преглед и премахване при необходимост поне веднъж в годината;
16. Мерки насочени към проследяване на достъпа и управление на инциденти.
 - 16.1. Система за създаване и поддържане на логове на достъпа до ресурсите с лични данни;
 - 16.2. Потребителите следва да бъдат информирани за поддържаните логове;
 - 16.3. Логовете не могат да бъдат достъпвани или променяни от неоторизиран персонал;
 - 16.4. Наличие на процедури за нотификация при пробив в сигурността на личните данни.
17. Мерки насочени към сигурността на работните станции.
 - 17.1. Използване само на лицензиран софтуер;
 - 17.2. Регулярно обновяване на антивирусните софтуери;
 - 17.3. Инсталирана софтуерна стена;
 - 17.4. Забрана за инсталиране на неоторизиран софтуер;
 - 17.5. Ограничаване използването на преносима памет;
 - 17.6. Процедури за автоматично заключване на сесиите;
 - 17.7. Редовно инсталиране на критични обновявания;
 - 17.8. Ограничаване използването на Интернет, а ако е невъзможно - използване на софтуери за филтриране на уеб страници и определени действия;
 - 17.9. Използване на стандартните опции за криптиране на дисковете за съхранение на информация на операционните системи;
 - 17.10. Взимане на съгласие преди интервенция от страна на администратора върху работната машина на потребителя.
18. Мерки насочени към сигурността на използваните мобилни устройства.
 - 18.1. Криптиране на мобилните устройства;
 - 18.2. Възможност за отдалечено проследяване на откраднато/загубено устройство;
 - 18.3. Регулярно създаване на резервни копия и синхронизация на данните;

**Политика за техническите и организационни мерки
за защита на личните данни**

- 18.4. Смартфоните изискват отключване посредством определено действие, свързано със сигурността.
19. Мерки, насочени към сигурността на вътрешната компютърна мрежа.
 - 19.1. Ограничаване мрежовите потоци само до най-необходимото;
 - 19.2. Осигуряване на достъп на мобилните изчислителни устройства посредством VPN;
 - 19.3. Отделяне на Wi-Fi мрежата от другите мрежи;
 - 19.4. Прилагане на WPA2 или WPA2-PSK за Wi-Fi мрежите;
 - 19.5. Провеждане на ежегодни тестове за проникване (външни).
20. Мерки, насочени към сигурността на сървърите.
 - 20.1. Ограничаване на достъпа до административни инструменти само заоторизирани лица;
 - 20.2. Незабавна инсталация на критични обновявания;
 - 20.3. Осигуряване на наличността на данните;
 - 20.4. Мерки насочени към сигурността на уеб страниците/уеб системи на институцията Използване на TLS протокол;
 - 20.5. Парола или потребителско име не се предават в URL;
 - 20.6. Категорийни данни, които могат да разкрият лични данни, не се предават в URL;
 - 20.7. Основните данни, които могат да послужат за разпознаване, са криптирани;
 - 20.8. Поставяне на банер за съгласие за бисквитките, които не са необходими за предоставяне на основните услуги.
21. Мерки, насочени към осигуряване на непрекъсваемостта на организационните процеси.
 - 21.1. Създаване на регулярни резервни копия;
 - 21.2. Съхранение на резервните копия на сигурно място;
 - 21.3. Планират се мерки за сигурност за предаване на резервните копия;
 - 21.4. Планиране и тестване на непрекъсваемостта на организационните процеси.
22. Мерки, насочени към осигуряване на сигурността на архивирането.
 - 22.1. Прилагане на специфични процедури за достъп до архивираните данни;
 - 22.2. Унищожаване на старите архиви по сигурен начин.
23. Мерки, насочени към осигуряване на мониторинг върху унищожаването на носители на данни.
 - 23.1. Записване на възможните интервенции в регистър;
 - 23.2. Наблюдаване на интервенциите на трети страни от официално лице на институцията;
 - 23.3. Изтриване на данните от носителя преди неговото унищожаване.
24. Мерки, насочени към контрол на доставчиците.
 - 24.1. Специални клаузи в договорите с доставчиците;
 - 24.2. Предвидени условия за връщане или унищожаване на данните;
 - 24.3. Контрол върху ефективността на предоставените гаранции (одити по сигурността, визити и т.н.).
25. Мерки, насочени към сигурността на обмен на данни с трети страни.
 - 25.1. Криптиране на данните преди тяхното изпращане;
 - 25.2. Предаване на секрета разделно и посредством различен канал;
 - 25.3. Изрична проверка, че е подаден верният получател;

Политика за техническите и организационни мерки за защита на личните данни

- 25.4. Прикачване на съобщение за конфиденциалност към всяко изпратено съобщение;
- 25.5. Използване само на служебни електронни пощи, когато съобщението се изпраща по имейл.
- 26. Мерки, насочени към физическата защита на помещенията
 - 26.1. Ограничаване на достъпа до помещенията посредством заключени врати;
 - 26.2. Инсталиране на аларма против взлом и периодичната им проверка;
 - 26.3. Използване на заключващи шкафове или каси за съхраняване на личните данни и/или преносимите изчислителни устройства;
 - 26.4. Следване на политика на „чисто бюро“.
- 27. Мерки, насочени към разработчици на електронни системи за институцията.
 - 27.1. Тестването на електронни системи се извършва само с фиктивни или анонимизирани данни;
 - 27.2. В случай на наличието на опционалности, насочени към поверителността на информацията, предлагане на настройки за тях на крайния потребител.
- 28. Мерки, в случай на необходимост от използване на криптографски услуги.
 - 28.1. Използване на признати алгоритми, софтуери и библиотеки;
 - 28.2. Запазване защитени секрета и криптографските ключове.

Раздел V. Трети страни, обработващи данни

29. В случай на използване на трети страни като обработващи данни, институцията използва само такива обработващи, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки за защита на личните данни. Тези мерки следва да бъдат сходни по обхват на тези, които са определени в раздел „Технически и организационни мерки за защита на личните данни“ от тази политика. Обработването се възлага чрез договор, в който изрично са посочени поне:
- 29.1. Предмет на обработването;
 - 29.2. Срок на обработването;
 - 29.3. Естеството и целта на обработването;
 - 29.4. Вида лични данни;
 - 29.5. Категориите субекти на данни;
 - 29.6. Задълженията и правата на администратора;
 - 29.7. Необходимостта от писмено разрешение от страна на институцията за използване на други обработващи от обработващия данни;
 - 29.8. Обработващият действа само по указания на администратора;
 - 29.9. Обработващият гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
 - 29.10. Обработващият подпомага администратора с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни.

Раздел VI. Обновяване на техническите и организационните мерки (ТОМ)

**Политика за техническите и организационни мерки
за защита на личните данни**

30. За целта на поддържане на ТОМ в актуално състояние с оглед на условията посочени в т.1.1-1.7, всяка година СЗД/ДЛЗД извършва преглед и при необходимост координира необходимостта от промени със засегнатите звена в институцията.

Директор:
Албена Мушкова



ИНСТРУКЦИЯ № 1 от 21 декември 2016 г.

за обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните данни, формата и начина на уведомяването

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. С тази инструкция се определят обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните им данни, формата и начина на уведомяването.

Чл. 2. Инструкцията се отнася до всички предприятия, които са вписани в публичния регистър на предприятията по чл. 33, ал. 1, т. 1 от Закона за електронните съобщения (ЗЕС), поддържан от Комисията за регулиране на съобщенията.

Глава втора

ОБСТОЯТЕЛСТВА, ПРИ КОИТО ПРЕДПРИЯТИЯТА, ПРЕДОСТАВЯЩИ ОБЩЕСТВЕНИ ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ УСЛУГИ, УВЕДОМЯВАТ ПОТРЕБИТЕЛИТЕ ЗА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 3. (1) В случай на нарушение на сигурността на личните данни по смисъла на § 1, т. 34а от допълнителните разпоредби на ЗЕС, което може да повлияе неблагоприятно на лични данни или на неприкосновеността на личния живот на абонат или на друго физическо лице, предприятието, при което е настъпило нарушението на сигурността, уведомява своевременно съответното лице за нарушението, но не по-късно от три дни от установяването му.

(2) Предприятието не уведомява абоната или друго физическо лице, в случай че Комисията за защита на личните данни (КЗЛД) е приела, че предприятието е предприело предхождащи подходящи технологични мерки за защита на сигурността на личните данни – обект на нарушението, при условията на чл. 261в, ал. 3 ЗЕС.

(3) В случаите по ал. 1 след разглеждане на възможните неблагоприятни последици от нарушението КЗЛД може да възложи на предприятието да уведоми съответните неуведомени засегнати лица по ал. 1.

Чл. 4. Извън случаите по чл. 3, ал. 2 предприятието не извършва уведомяване и когато са налице обстоятелствата по чл. 3, параграф 5 от Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации.

Чл. 5. При определянето, че дадено нарушение на сигурността на личните данни може да повлияе неблагоприятно на лични данни или на неприкосновеността на личния живот на абонат или на друго физическо лице, предприятието отчита следните обстоятелства:

1. категориите лични данни – обект на нарушение на сигурността, като данни по чл. 5, ал. 1 от Закона за защита на личните данни; данни по чл. 248, ал. 2 ЗЕС; данни

по чл. 3, параграф 2, буква „а“ от Регламент (ЕС) № 611/2013; данни в широкомащабни регистри на лични данни по смисъла на Наредба № 1 от 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни на КЗЛД и данни за лица, заемащи висши държавни и други длъжности по смисъла на Закона за публичност на имуществото на лица, заемащи висши държавни и други длъжности; биометрични данни по смисъла на чл. 4, т. 14 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (общ регламент относно защитата на данните); данни, чието обработване съгласно решение на КЗЛД застрашава правата и законните интереси на физическите лица;

2. характера на нарушението на сигурността на личните данни и вероятните последици от него за засегнатия абонат или друго физическо лице като някоя от последиците, посочени в чл. 3, параграф 2, буква „б“ от Регламент (ЕС) № 611/2013; загуба на данни; незаконно унищожаване; нерегламентиран достъп; трайни здравословни увреждания или смърт на група физически лица или на отделно физическо лице по смисъла на Наредба № 1 от 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни на КЗЛД.

Глава трета

ФОРМА И НАЧИН НА УВЕДОМЯВАНЕ

Чл. 6. Предприятието уведомява абоната или друго физическо лице за настъпилото нарушение на сигурността на личните данни в разбираема форма. Уведомлението задължително съдържа информацията по Приложение II от Регламент (ЕС) № 611/2013.

Чл. 7. При спазване на изискванията на чл. 3, параграф 6 от Регламент (ЕС) № 611/2013 предприятието уведомява абоната или друго физическо лице чрез средства за комуникация, гарантиращи незабавното получаване на информацията по чл. 6.

Чл. 8. (1) В случаите по чл. 3, параграф 7 от Регламент (ЕС) № 611/2013 предприятието прави обявление в две или повече национални и/или регионални медии. Обявлението в този случай е в срока по чл. 3.

(2) След идентифициране на всички засегнати от нарушението лица предприятието незабавно уведомява всяко от тях, като им предоставя информацията по чл. 6, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Тази инструкция е приета на основание чл. 261г, ал. 1 ЗЕС с решение на КЗЛД от 21.12.2016 г.

§ 2. Инструкцията влиза в сила три дни след обнародването ѝ в „Държавен вестник“.

Председател: **Венцислав Караджов**

Приложение II Списък на лицата, които обработват лични данни

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян

Приложение II

2. Списък на лицата, обработващи лични данни
(към Регистър на лицата, които обработват лични данни)

1. СПИСЪК НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Наименование/Инициали/Реф. номер	Длъжност/и	От	До
Светла Башова	Главен счетоводител	15.09.2020 г.	15.09.2021 г.
Десислава Дрянкова	Ръководител ИКТ	15.09.2020 г.	15.09.2021 г.
Албена Мушкова	директор	15.09.2020 г.	15.09.2021 г.

Към Приложение II - Регистър на лицата, които обработват лични данни

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл.
Смолян

Регистър на лицата, които обработват лични данни

Данни за администратора

Администратор	СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян
Адрес	Ул. „П. Яворов“ 4
Име, фамилия на директора	Албена Мушкова
E-mail	Sou_starcevo@abv.bg
Телефон	03073/2084; 0888861762

Коментари

1. Този регистър следва да се разглежда като приложение към регистъра на дейностите по обработване на лични данни.
2. В регистъра са посочени длъжности/позиции в институцията, ангажирани с обработването на лични данни.
3. Конкретните лица, заемащи отделните длъжности, са посочени в Списък на лицата, обработващи лични данни

РЕГИСТЪР¹

Дейности по обработване на данни	Длъжност/и
Реализиране на трудови правоотношения със служители на институцията	
Провеждане на конкурси за назначаване на нови служители	
Контрол на работната среда и изпълнение на служебните задължения	
Спазване на законови задължения (напр. ОРЗД)	
Осъществяване на образователния процес	
Създаване на подходяща и здравословна среда в образователната институция	
Осигуряване на обща и/или на допълнителна подкрепа за деца/ученици	

¹ Дейностите следва да съответстват на посоченото в Регистъра на дейности по обработване на лични данни

Към Приложение II - Регистър на лицата, които обработват лични данни

Здравно осигуряване на лица над 18г.	
Получаване на дарения	
Осъществяване на контакт с родител	
Фото и видеоматериали, свързани с дейността на институцията	

Към Приложение I – Регистър на категории дейности по обработването (обобщаващ)

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян
Регистър на категории дейности по обработването (обобщаващ)

Данни за обработващия

Обработващ	Светла Башова, СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян
Адрес	Ул. „П.Яворов“ 4
Мейл	Sou_starcevo@abv.bg
Телефон	0888861762
ДЛЗД	Десислава Джандева - Дрянкова

Администратор	Категории дейности	Предаване на лични данни на трета държава или международна институция,	Прилагани технически и организационни мерки (ТОМ)
МОН/РУО	Информация за персонала Данни на персонал на институцията: Лични данни, включващи ЕГН, адрес, имена, трудов стаж, заплатата, месторождение, образование, квалификация.	Не	Съгласно получени насоки от администратора на данни
МОН/РУО	Информация във връзка	Не	Съгласно получени насоки от администратора на

Към Приложение I – Регистър на категории дейности по обработването (обобщаващ)

Администратор	Категории дейности	Предаване на лични данни на трета държава или международна институция,	Прилагани технически и организационни мерки (ТОМ)
	с образователния процес Данни на ученици: Данни за изпити Документи за завършен клас, етап, степен, придобита професионална квалификация и/или правоспособност Данни от електронен дневник Данни за социален статус на дете/ученик		данни
Община	Прием/записване на деца/ученици Данни за приемни изпити/записване	Не	Съгласно получени насоки от администратора на данни
Социално подпомагане	Информация за предоставяне на социални помощи. Данни за	Не	Съгласно получени насоки от администратора на данни

Към Приложение I – Регистър на категории дейности по обработването (обобщаващ)

Администратор	Категории дейности	Предаване на лични данни на трета държава или международна институция,	Прилагани технически и организационни мерки (ТОМ)
	присъствия/отсъствия на деца		
Други (Следва да се уточнят в зависимост от конкретния случай)			Съгласно получени насоки от администратора на данни

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Приложение I

към раздел VIII, т. 24, I. Регистър на дейности
по обработване на лични данни

1. Регистър на дейности по обработване на лични данни (администратор)

Данни за администратора

Администратор	СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“, с. Старцево, общ. Златоград, обл. Смолян
Адрес	Ул. "П.Яворов" 4
Име, фамилия на директора	Албена Мушкова
Мейл	Sou_starcevo@abv.bg
Телефон	03073/2084; 0888861762
ДЛЗД	Десислава Джандева - Дрянкова D_djandeva@abv.bg

РЕГИСТЪР

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
Реализиране на трудови правоотношения със служители на институцията	Служители Бивши служители (напр. напуснали,	Общи персонални данни Данни за контакт	Служители на институцията Обработващи	Съгласно приложимите нормативни актове*	Съгласно политика за ТОМ на институцията	Законово задължение (Кодекс на труда, ДПК, КСО)

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
	пенсионирани лица)	Данни за пенсионни, осигурителни и данъчни права и задължения (вкл. ползване на отпуски)	данни			Съгласие на лицето (за изплащане на заплатата по банков път)
		Данни за синдикална принадлежност	Публични институции			Договорно задължение
		Финансови данни (вкл. изплатена сума, банкова сметка, допълнително материално стимулиране)	Финансови организации			
		Данни за образование,				

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
		квалификация, професионален опит; Данни за изпълнение на трудовите задължения (оценка на изпълнението; повишаване на квалификацията)				
Провеждане на конкурси за назначаване на нови служители	Кандидати за работа в институцията	Общи персонални данни Данни за контакт; Данни за образование, квалификация, професионален опит;	Служители на институцията Обработващи данни	До приключване на съответния конкурс и избор на кандидат, но не по дълъг от три години	Съгласно политика за ТОМ на институцията	Легитимен интерес на работодателя Съгласие на кандидата Пред-договорни отношения

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
Контрол над чувствителни зони и ресурси на институцията	Служители	Видеонаблюдение	Служители на институцията	Съгласно приложимите нормативни актове***	Съгласно политика за ТОМ на институцията	Легитимен интерес на работодателя
	Посетители		Обработващи данни	(видеонаблюдение)		Изпълнение на задача в обществен интерес
	Ученици/Деца					
	Родители/Настойници					
Спазване на законови задължения (напр. ОРЗД)	Служители	Общи персонални данни	Служители на институцията	Няма определен период	Съгласно политика за ТОМ на институцията	Законово задължение
		Системни действия	Надзорен орган (напр. КЗЈД)			
Осъществяване на образователен процес	Ученици/Деца	Персонални данни	Служители на институцията	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Законово задължение
	Родители/Настойници	Данни за контакт	Публични институции	Наредба № 8/2016 г. за информацият		(ЗПУО, ЗПОО, ДОС, други)
		Данни за				

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
		присъствия, отсъствия, успех, положени изпити	Други организации от същата категория (напр. други училища, детски градини)	а и документите в СПУО и др.		
		Фотографии				
		Изплатени стипендии	Самите лица, чиито данни се обработват			
		Видеозаписи от ДЗИ	Обработващи данни			
Създаване на подходяща и здравословна среда в образователната институция	Ученици/Деца Родители/Настойници	Персонални данни Данни за контакт СОП	Служители на институцията Публични институции Други организации от	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Законово задължение

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
		Здравни / медицински данни	същата категория (напр. други училища, детски градини)			
			Самите лица, чиито данни се обработват			
			Обработващи данни			
Осъществяване на обща и/или на допълнителна подкрепа	Ученици/Деца Родители/Настойници	Персонални данни Данни за контакт Деца/ученици, в т.ч. за допълнителната подкрепа деца/ученици: - в риск; - със СОП; - с изявени дарби; - с хронични	Служители на институцията Публични институции Други организации от същата категория (напр. други училища, детски градини, ЦСОП, РЦППО)	Съгласно ЗПУО, ЗПОО, Наредба за приобщаващо образование и Наредба № 8/2016 г. за информацията и документите	Съгласно политика за ТОМ на институцията	Законово задължение

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
		заболявания. Здравни / медицински данни	Самите лица, чиито данни се обработват Обработващи данни			
Здравно осигуряване на лица над 18г.	Лица, над 18г. (ученици)	Персонални данни	Служители на институцията Публични институции (НАП)	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Законово задължение
			Самите лица, чиито данни се обработват Обработващи данни			

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
Получаване на дарения	Дарители на институцията	Персонални данни	Служители на институцията Самите лица, чиито данни се обработват Обработващи данни	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Законово задължение
Осъществяване на контакт с родител	Родители/Настойници /Други роднини	Персонални данни, Данни за контакт	Служители на институцията Самите лица, чиито данни се обработват Обработващи данни	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Съгласие
Фото и видеоматериали, свързани с	Деца/Ученици	Фотографии	Служители на институцията	Съгласно приложимите нормативни актове	Съгласно политика за ТОМ на институцията	Съгласие

Приложение I Регистър на дейностите по обработване на лични данни (администратор)

Цел на обработването	Категория лица	Категории лични данни	Категории получатели на данните	Период на съхранение	Прилагани ТОМ	Основание за обработване на данните
дейността на институцията		Видеозаписи	Самите лица, чиито данни се обработват и техните родители	актове	институцията	
			Обработващи данни			

Относно приложими нормативни актове (списъкът може да се допълни от институцията):

*Съгласно Данъчно-осигурителен процесуален кодекс:

- вестомости за заплати - 50 години
- счетоводни регистри и финансови отчети - 10 години
- документи за данъчно-осигурителен контрол - 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани
- всички останали носители - 5 години.

**Съгласно Кодекс на труда:

- съгласно давността за налагане на дисциплинарни наказания до 1 година от извършването му.

***Закон за частната охранителна дейност:

- 30-дневен срок след извършването им.
-

СРЕДНО УЧИЛИЩЕ „СВЕТИ КНЯЗ БОРИС I“,
С. Старцево, общ. Златоград, обл. Смолян

**Инструкция за използването на информационните
системи от служителите**

Раздел I. Общи положения

Чл. 1. (1) Инструкцията за използване на информационните системи информира педагогическите специалисти и непедagogическия персонал за правата и задълженията им по отношение на използването нейното приложение и използване.

(2) Инструкцията определя правилата за използване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на родители и учители, за администриране, свързано с учебно-възпитателния процес, а също така е средство за извършване на проучвания и обмяна на информация.

(3) Достъпът до данните в локалната мрежа и ползването на програмните продукти на институцията от педагогическите специалисти и непедagogическия персонал е необходимо с оглед ефективното изпълнение на отговорностите и задълженията.

Чл. 2. Информационните технологии включват локалните мрежи, интернет, електронната поща и всички програмни продукти, които институцията притежава и ползва.

Чл. 3. Инструкцията дава указания за начина на употреба от педагогическите специалисти и непедagogическия персонал на информационните технологии, насърчава ползването им с цел увеличаване на продуктивността и ефективността на работата.

Чл. 4. (1) Определеният заместник-директор, ръководителят на направление „Информационни и комуникационни технологии“/специалистът по ИТ технологии в институцията са отговорни за цялостната дейност на информационните технологии и за подпомагането работата на служителите на институцията с тях.

(2) При съмнение за нарушение на сигурността на личните данни, лицето, което е установило несъответствието (случайно или неправомерно унищожаване на лични данни, загуба, промяна, неразрешено разкриване или нерегламентиран достъп, незабавно уведомява лицата по ал. 1 и определения служител по защита на личните данни за предприемане на действия по прилагане на Инструкцията за действие при пробив в сигурността.

Чл. 5. Служителите в институцията са задължени да спазват правилата, определени с настоящата Инструкция.

Чл. 6. Всички компютърни програмни продукти и информация, създадена и съхранена от служителите, са собственост на институцията.

Чл. 7. Служителите в институцията нямат право да вземат програмните продукти с цел инсталирането им на домашните им компютри и преносими устройства, с изключение на електронните учебници и създадените за он-лайн обучение софтуери.

Чл. 8. При напускане на институцията служителите нямат право да копират

или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Раздел II. Контрол върху работата с информационните технологии

Чл. 9. (1) Ръководството на институцията има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от служителите в институцията.

(2) Ръководството на институцията, включително и определеното длъжностно лице по защита на личните данни, имат право да проверява изцяло служебните компютри, предоставени за учебни цели на служителите в институцията, както и техниката, която ползват учители и служители във връзка с изпълнение на служебните им задължения.

Раздел III. Конфиденциалност

Чл. 10. Резултатите от извършения контрол върху работата с информационните технологии на институцията се считат за конфиденциални и не се разгласяват от ръководството.

Раздел IV. Допустимо ползване на информационните технологии за лични цели

Чл. 11. Учебните информационни системи са предназначени за ползване при изпълняване на служебните задължения на служителите.

Чл. 12. Тези системи могат да се ползват и за лични цели при следните условия:

1. Това е инцидентно, рядко и за кратко време.
2. Не е по време на работа, а е в извънработно време.
3. Това не пречи на работата на останалите служители. В това число се включват дейности, които могат да доведат до конфликт на интереси.
4. Това не води до допълнителни разходи за институцията.

(Изброяването не е изчерпателно и може да бъде допълнено с цел постигане на съответствие с Общия регламент за защита на личните данни № ЕС 2016/679 от 27 април 2016 г. на Европейския парламент и на Съвета.)

Раздел V. Забрани за ползване на информационните технологии

Чл. 13. Забранява се ползването на компютърните и информационните системи на институцията в следните случаи:

1. Заобикаляне на системите за сигурност, с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на информационните ресурси за извършване на нерегламентирана дейност.
3. Използване на ресурсите за подпомагане дейността на външни организации, техните продукти, услуги или бизнес практика, с цел облага.
4. Електронна поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.
5. Ползването на компютърните системи за политическа дейност, която пряко

- или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, прашани от служители на институцията трябва да са лично подписани и да са до точно определен брой адресати, които са дали съгласие за използване на електронния им адрес.
 7. Свалянето от Интернет на аудио и видео файлове и други.
 8. Сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти.
 9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

(Този списък на забранените дейности във връзка с информационните технологии не е изчерпателен. Към него може да се добавя допълнителни забрани, като се актуализира настоящата Инструкция и се утвърди със заповед на директора.)

Раздел VI. Разкриване на информация

Чл. 14. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за институцията и накърняване на нейния имидж и репутация.

(2) Служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имущественна отговорност по КТ.

Раздел VII. Антивирусна защита

Чл. 15. (1) Компютърните вируси са голяма заплаха за всички потребители на IT услуги и служителите трябва да имат необходимите знания как вирусите се разпространяват, каква вреда могат да нанесат и как да се предпазват от тях.

(2) Компютърният вирус е компютърна програма, която се задейства на даден компютър и се разпространява към другите дискове и програми, които са в контакт със заразенения компютър.

(3) Вирусът може да причини блокиране на компютъра, да промени бази данни, да направи някои данни невъзможни за ползване и даже да форматира диск и така да се загуби цялата информация на тях.

Раздел VIII. Организация на защитата от вируси

Чл. 16. (1) IT специалиста на институцията носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява поне веднъж седмично с най-новата версия.

(2) Служителите трябва да приемат всяко съобщение за вирус изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които служителят знае, че са заразени е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на вирусна атака служителят трябва незабавно да информира IT специалист без да предприема никакви действия самостоятелно.

(5) На служителите е разрешено да свалят файлове от външни източници на мрежата на институцията във връзка с тяхната работа. Не е разрешено на служителите да се инсталират програмни продукти без предварителното разрешение на IT специалиста, тъй като има опасност от заразяване с вируси.

(6) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена с вируси. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(7) Електронни писма, получени от неизвестни податели трябва да се изтриват и в никакъв случай да не се отварят файлове, прикачени към тях.

(8) Файлове, получени от неизвестни податели трябва да се трият без да се отварят.

(9) Ползването на външни носители (дискове, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Раздел IX. Архивиране на информацията

Чл. 17. (1) Сривовете в компютърното оборудване, вирусите, случайното изтриване на файлове могат да причинят загуба на данни, поради което е необходимо информацията във всяка компютърна система да бъде архивирана.

(2) Целта на архивирането и възстановяването е да се възстанови работата възможно най-бързо в случай на прекъсване по технически причини. По този начин се минимизират възможните проблеми и загуби.

(3) Служителите в институцията, съгласувайки с IT специалиста, трябва да имат адекватна система за архивиране на данните от своята работа на технически носители (дискове, USB и др.).

(4) Честотата на архивирането се определя от директора в писмена процедура и зависи от броя транзакции и тяхната значимост за системата.

(5) Задължително архив (архивиране на файлове) се прави веднъж месечно.

Раздел X. Достъп и пароли

Чл. 18. (1) Служителите получават достъп до локалната мрежа и до всички програми, необходими за изпълнение на служебните им задължения.

(2) Достъпът до дадена програма се дава на конкретен служител и не може да се прехвърля на друг.

(3) Служителите трябва да пазят своите лични пароли в тайна.

Чл. 19. Когато даден продукт изисква парола трябва да спазват следните правила:

1. служителите трябва да променят първоначалната парола (обикновено генерирана от програмния продукт) като измислят своя индивидуална при първото влизане в съответната информационна система;
2. паролите трябва да са с не по-малко от 5 знака;
3. паролите трябва лесно да се помнят, за да не се налага да бъдат записвани на хартия;
4. паролите не трябва да са лесни за отгатване от колегите;
5. паролите не трябва да се споделят с колеги или други познат;
6. паролите не трябва да се записват на хартия и да се оставят на работното

място;

7. ако е необходимо паролите могат да се сменят на определена честота (всеки 3, 6, 12 месеца);
8. при 3 неуспешни опита за влизане в дадена програма достъпът може да бъде блокиран;
9. при периодична промяна на паролата не трябва да се използват вече използвани пароли;
10. системите не трябва да позволяват един и същи потребител да се включи в няколко компютъра едновременно с една и съща парола.

Чл. 20. Ако забравят своята парола служителите трябва незабавно да уведомят оторизирания помощник директор и да се свържат с IT специалист.

Раздел XI. Интернет

Чл. 21. (1) Ръководството насърчава ползването на Интернет от служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за уместната употреба на Интернет от служителите на институцията.

(3) Свалянето от Интернет на аудио или видео файлове е забранено. Не е разрешено и свалянето на програмни продукти от Интернет без предварителното одобрение на компютърен специалист.

Раздел XII. Електронна поща

Чл. 22. (1) Електронната поща на институцията не може да се ползва за комерсиални цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на институцията.

(2) Ползването на електронната поща за политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат също не се позволява.

(3) Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност се забранява. Всички електронни писма, изпращани от служителите трябва да са лично подписани.

(4) Неформалните съобщения, които не са от официален характер трябва да се трият от пощата, за да не се товарят сървърите на институцията.

(5) Всички електронни писма и важни съобщения, които имат отношение към дейността на училището, трябва да се принтират и представят за завеждане с входящ номер в дневника за входяща кореспонденция от определеното длъжностно лице, като екземпляр се съхранява в съответните класьор и в електронната поща.

(6) Служителите трябва да проверяват внимателно точния адрес на получателите на официални писма, особено такива с прикачени файлове, за да не се допусне получаване на информация от чужди лица.

Раздел XIII. Лице за контакт

Чл. 23. Всички технически въпроси във връзка с работата на компютърните системи се насочват към IT специалист на институцията или към друго лице, определено от директора.

Допълнителни разпоредби

§ 1. При извършване на самооценката на вътрешните контроли следва да се направи анализ и оценка на риска на критичните информационни системи в институцията.

§ 2. Целта е да се идентифицират най-важните компоненти (оборудване, програми, бази данни), заплахата за тяхната повреда или загуба, последиците от това за дейността на институцията налични контроли за да се предотвратят потенциалните проблеми и допълнителни контроли, които са необходими за подобряване на системата.

§ 3. Оценката на риска обхваща извършеното, както и моментното състояние, мерките за подобряване на слабите места във вътрешните контроли, необходимите ресурси и остатъчният риск за институцията, който контролите няма как да елиминират.

§ 4. При създаването на програмен продукт специално за нуждите на институцията е необходимо още при задаването на неговите параметри на доставчика да се зложат основните контролни функции, които този продукт трябва да има.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Инструкцията влиза в сила утвърждаването ѝ със Заповед № *PO-07-18*/28/20*20* г. на директора.

Директор:

Албена Мушкова

