Утвърдил:………………

............................................

*Директор на .................................*

**ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА РЕГИСТЪР „ПЕРСОНАЛ“**

**В ................................................**

|  |
| --- |
| **ОБЩО ОПИСАНИЕ НА РЕГИСТЪР „ПЕРСОНАЛ“** |
| Регистърът съдържа следните категории лични данни:  **Физическа идентичност** – 1. физическата идентичност - име, ЕГН, адрес, данни от л.к. месторождение, телефони за връзка и банкови сметки;  2. психологическа идентичност - документи относно психическото здраве;  3. социална идентичност - образование и трудова дейност;  4. семейна идентичност - семейно положение и родствени връзки;  5. лични данни, които се отнасят до здравето;  6. други - лични данни относно гражданско-правния статус на лицата. |
| **ЦЕЛ И ОСНОВАНИЕ ЗА СЪБИРАНЕ НА ЛИЧНИ ДАННИ В РЕГИСТЪР „ПЕРСОНАЛ“** |
| Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване,  Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право. |
| **ТЕХНОЛОГИЧНО ОПИСАНИЕ НА РЕГИСТЪР „ПЕРСОНАЛ“** |
| Личните данни постъпват на   * На хартиен носител   Срок на съхранение – съгласно Номенклатурата на делата в институцията със срокове на съхранение; |
| **ДЛЪЖНОСТИ, КОИТО ОБРАБОТВАТ ЛИЧНИТЕ ДАННИ ОТ РЕГИСТЪР „ПЕРСОНАЛ“** |
| Директор ,гл.счетоводител ,ЗАС и касиер. |
| **ДЛЪЖНОСТИ, КОИТО ИМАТ ДОСТЪП ДО ЛИЧНИТЕ ДАННИ ОТ РЕГИСТЪР „ПЕРСОНАЛ“** |
| Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения, а именно: директор, гл.счетоводител,ЗАС и касиер. |
| **НИВО НА ВЪЗДЕЙСТВИЕ НА РЕГИСТЪР „ПЕРСОНАЛ“** |
| Поверителност – ниска  Цялостност – ниска  Наличност – ниска  Общо за регистъра - ниска |
| **ОРГАНИЗАЦИОННИ МЕРКИ ЗА ФИЗИЧЕСКА ЗАЩИТА** |
| определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа. |
| **ТЕХНИЧЕСКИ МЕРКИ ЗА ФИЗИЧЕСКА ЗАЩИТА** |
| включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.  Трудовите досиета на персонала не се изнасят извън сградата на институцията.  Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител. |
| **МЕРКИ ЗА ЗАЩИТА НА ЕЛЕКТРОННИ ДАННИ** |
| Лични данни на служители се обработват със специализиран счетоводен софтуер. При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на институцията.  При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване. |
| **ЗАЩИТА ПРИ ИЗВЪНРЕДНИ СИТУАЦИИ** |
| Учебното заведение има разработен Авариен план за действие при извънредни ситуации и Противопожарни правила. Взети са мерки за защита – осигурени са пожарогасителни средства. Служителите са преминали инструктаж.  В случай на регистриран неправомерен достъп до личните данни на служителите Длъжностното лице за защита на личните данни информира засегнатите лица в 3 дневен срок от констатирането на неправомерния достъп в писмен вид чрез „**Уведомление до субектите на данни за нарушение на сигурността на личните данни“** |
| **ДОСТЪП ОТ ТРЕТИ СТРАНИ** |
| Досиетата на служителите не се изнасят и не се предоставят вцялостен вид на трети страни. Отделни категории лични данни се предоставят на трети страни както следва:   * **Служба по трудова медицина –** лични данни за здравословно състояние**;** * **Застрахователни компании –** лични данни, необходими за сключване на договор „Трудова злополука“.   Предоставянето на данните е на хартиен носител при спазване на мерки за конфиденциалност – затворени в непрозрачен запечатан плик. |
| **УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ ОТ РЕГИСТЪР „ПЕРСОНАЛ“** |
| Унищожаване на документи с лични данни, за които не се изисква предаване в Държавен архив, изтекли са законови или други определени срокове за съхранение. Унищожаването се извършва от определен със заповед на учебното заведение служител и се документира в писмено. Данните на хартия се унищожават чрез нарязване с шредер или изгаряне. |
| **ПРЕДОСТАВЯНЕ НА ДОСТЪП НА СЛУЖИТЕЛИТЕ ДО ТЕХНИ ЛИЧНИ ДАННИ. ДОПЪЛВАНЕ И УНИЩОЖАВАНЕ** |
| Служителите могат да получат информация/справка за обработваните свои лични данни устно от гр.счетоводителя и ЗАС. При необходимост служителя предоставя допълнителна информация за променени лични данни на посочените лица.  Искане за унищожаване на лични данни могат да подават и бивши служители като попълнят искане в свободен текст. Длъжностното лице за защита на личните данни дава отговор в 14 дневен срок. |