Професионална гимназия по селско стопанство
гр. Нова Загора, ул.Цар Освободител №67, 0457/62757,pgss@abv.bg

Утвърдил:
/Директор – Лиляна Стоянова/

ИНСТРУКЦИЯ
ЗА ПРИЛАГАНЕ НА ПОДХОДЯЩИ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
в Професионална гимназия по селско стопанство

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата инструкция определя подходящи технически и организационни мерки за защита на личните данни и правилата за тяхното прилагане при обработване на лични данни от Професионална гимназия по селско стопанство

Чл. 2. Инструкцията има за цел да гарантира правата и свободите на физическите лица във връзка с обработване на личните им данни и съответствието на обработването на лични данни с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), Закона за защита на личните данни и други нормативни изисквания във връзка с обработването на лични данни.

Чл. 3. Прилаганите технически и организационни мерки са задължителни за всички служители на Професионална гимназия по селско стопанство, както и за всички други лица, които изпълняват задачи или договори, възложени от или изпълнявани в Професионална гимназия по селско стопанство, при които се обработват лични данни.

Чл. 4. Подходящите технически и организационни мерки за защита на личните данни се определят въз основа на анализ на риска, извършен въз основа на следните фактори:
1. естеството, обхвата, контекста и целите на обработването;
2. рисковете с различна вероятност и тежест за правата и свободите на физическите лица;
3. достиженията на техническия прогрес;
4. разходите за прилагане.

Чл. 5. Прилаганите технически и организационни мерки се разпределят в следните видове защита:
1. мерки за персонална защита;
2. мерки за физическа защита;
3. мерки за документална защита;
4. мерки за защита на автоматизирани информационни системи и криптографска защита.

Чл. 6. (1) Прилаганите технически и организационни мерки се преценяват периодично с оглед способността им да гарантират постоянна поверителност, цялостност, наличност и устойчивост на системите и дейностите по обработване на лични данни, като подлежат на редовно изпитване и оценка на ефективността.

(2) Длъжностното лице по защита на данните подпомага администратора по ал. 1, като наблюдава спазването на нормативни изисквания за защита на личните данни и изисквания, произтичащи от вътрешни правила, политики и процедури на администратора, включително като повишава осведомеността и обучението на персонала, участващ в операциите по обработване.

II. МЕРКИ ЗА ПЕРСОНАЛНА ЗАЩИТА

Чл. 7. Персоналната защита на личните данни включва следните организационни мерки:

1. определяне на длъжностите и задачите, които имат достъп и обработват лични данни;
2. определяне на отговорниците за достъп до регистрите с лични данни;
3. спазване на принципа „необходимост да се знае“ от всяко лице под ръководството на администратора, което има достъп до лични данни;
4. обработване на лични данни само по указание на администратора, освен ако обработването не се изисква от задължение, произтичащо от правото на Европейския съюз и от българското законодателство;
5. периодично обучение на служителите на администратора, които обработват лични данни, включително тренировки за действия при инциденти, свързани със защитата на личните данни и познаване на процедура за действия при нарушения на сигурността на личните данни.

Чл. 8. Служителите на администратора имат оторизиран достъп само до тези регистри, които са необходими за изпълняване на техните задължения или конкретно възложени задачи.

III. МЕРКИ ЗА ФИЗИЧЕСКА ЗАЩИТА

Чл. 9. Организационните мерки за физическа защита включват:

1. определяне на зоните с контролиран достъп, в които се съхраняват лични данни, както следва - /трудови досиета, ученически досиета, финансово-счетоводна и друга документация, в която се съдържат лични данни/
2. физически достъп до зоните с контролиран достъп да се осигурява само на оторизирани служители, като се предотвратява нерегламентиран достъп до лични данни
3. определяне на екип за реагиране при нарушения на сигурността на личните данни

Чл. 10. Техническите мерки за физическа защита включват:

1. ключалки на помещения, в които се съхраняват лични данни, които се заключват, ако в тях няма отговорен служител;
2. шкафове за съхранение на лични данни, които се заключват, ако в съответното помещение няма отговорен служител;
3. устройства за контрол на физическия достъп;
4. охрана на сградата на Професионална гимназия по селско стопанство, осъществявана с физическа охрана при влизане в сградата и с видеонаблюдение в коридорите на сградата;
5. пожароизвестителна система;
6. други мерки

IV. МЕРКИ ЗА ДОКУМЕНТАЛНА ЗАЩИТА

Чл. 11. Мерките за документална защита на личните данни се отнасят до регистрите с лични данни, обработвани на хартиен носител, като включват:

1. определяне на регистрите с лични данни, които се обработват на хартиен носител, както следва - регистър „Човешки ресурси“, регистър „Ученици“

2. осигуряване на достъп до личните данни в съответния регистър от лицето, отговорно за достъпа до данните в регистъра, включително под формата на справки, извлечения, копия от документи и други подобни;

3. спазване на сроковете за съхранение на личните данни;

4. своевременно предприемане на действия по унищожаване на лични данни след изтичане на срока за съхранение и преценка за изпълнението на целите на обработването на лични данни;

5. документиране на унищожаването на лични данни;

6. извършване на проверки и контрол за спазване на установените мерки.

V. МЕРКИ ЗА ЗАЩИТА НА АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ И КРИПТОГРАФСКА ЗАЩИТА

Чл. 12. Администраторът осигурява контролиран достъп на служителите при обработване на лични данни във връзка с:

1. техническите и програмно-информационните ресурси, използвани при обработката и защитата на личните данни;

2. информационните носители и извършваните действия по тяхното регистриране, преместване, подреждане, копиране, преобразуване и друг вид обработка;

3. личните данни в регистрите, както и контрол на лицата, извършващи действия по обработване на личните данни съгласно предоставените им права;

4. разполагането, поддържането и преместването на техническите ресурси, използвани за обработка на личните данни.

Чл. 13. Архивното копие и процедурите за възстановяване на данни се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните.

Чл. 14. Защитата на автоматизираните информационни системи включва тяхното администриране, при отчитане на следните изисквания:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

2. администраторските профили са персонални;

3. администраторските профили се използват само за административни цели;

4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

6. данните за автентикацията на администраторските акаунти:

а) са различни за всяка система;

б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;

в) се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран служител;

7. поддържате на списък на администраторските профили за автоматизираните информационни системи и техните компоненти;

8. годишен преглед на администраторските профили с цел удостоверяване на актуалността им;

9. задължителна смяна на пароли периодично (най-малко веднъж годишно), при прекратяване на договорните отношения със служители или трети срани, на които те са били известни и при констатиране на нарушения на сигурността на личните данни.

Чл. 15. Забранява се ползването на компютърните и информационните системи на Професионална гимназия по селско стопанство в следните случаи:

1. ползване на информационните ресурси за извършване на нерегламентирана дейност;

2. използване на ресурсите за подпомагане дейността на външни организации, техните продукти, услуги или бизнес практика, с цел облага;

3. електронна поща на институцията не може да се ползва за комерсиални лични цели, политически цели, религиозни цели или да се подпомага дейност, която не е свързан с дейността на институцията;

4. подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от служители на институцията трябва да са лично подписани и да са до точно определен брой адресати;

5. свалянето от Интернет на аудио и видео файлове и други.

6. сваляне и инсталиране на компютърни програми от Интернет без разрешение на компютърните специалисти и без нужния лиценз, ако се изисква такъв;

7. копиране на лицензираните компютърни програми на институцията с цел лична употреба;

8. споделяне на пароли или възпроизвеждането им по друг нерегламентиран начин.

Чл. 16. Когато дадена информационна система или продукт изискват парола, се спазват най-малко следните мерки:

1. служителите 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 десет 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 се споделят с колеги или други познат и не се възпроизвеждат по нерегламентиран начин;

6. ако е необходимо, паролите се променят на определени периоди (всеки 3, 6, 12 месеца);

7. при 3 неуспешни опита за влизане в дадена програма достъпът може да бъде блокиран;

8. при периодична промяна на паролата не трябва да се използват вече използвани пароли;

9. системите не трябва да позволяват един и същи потребител да се включи в няколко компютъра едновременно с една и съща парола.

Чл. 17. Ако забравят своята парола служителите трябва незабавно да уведомят оторизирания помощник директор и да се свържат с отговорния служител на Професионална гимназия по селско стопанство

Чл. 18. (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.

Чл. 19. 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 софтуери за онлайн обучение.

Чл. 20. При напускане на институцията служителите нямат право да копират или изтриват/унищожават файлове с данни, които са създадени във връзка с тяхната работа.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Инструкцията е приета на основание чл. 24, пар. 1 и 2 и чл. 29 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

§ 2. Инструкцията е утвърдена със Заповед № РД 07 - 1432/14.09.2022 г. на директора на Професионална гимназия по селско стопанство.