„ПЪРВО ЧАСТНО ОСНОВНО УЧИЛИЩЕ“ ООД

ИНСТРУКЦИЯ ЗА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

УТВЪРЖДАВАМ:

СТАНЧО СЛАВОВ
УПРАВИТЕЛ

БУРГАС, 23.05.2018 г.

Съдържание

1. Определения на използваните понятия

Дружество	„ПЪРВО ЧАСТНО ОСНОВНО УЧИЛИЩЕ“ ООД„ ЕИК 204628969, със седалище и адрес на управление ул. „Антим I“, № 24, гр. Бургас, което е работодател на всеки от служителите, нает въз основа на Трудов договор.
Пряк ръководител	Представител на Дружеството, който е посочен в Трудовия договор на съответния Служител или назначен със заповед на Дружеството за пряк ръководител на Служителя.
Служител	Физическо лице, нает от Дружеството.
Ръководство	Управител на Дружеството, директор на училището и/или всяко друго лице в Дружеството, на което са предоставени ръководни функции и управленска власт.
Инструкция	Настоящата Инструкция за сигурност на информацията.
Трета страна	Физическо лице, юридическо лице или друг субект, необвързан с Дружеството.

2. Цел и обхват

2.1. Системата за сигурност на информацията в Дружеството има за цел да защитава Служителите, партньорите и клиентите на Дружеството от незаконни или вредни действия на физически лица, пряко или косвено, съзнателно или несъзнателно при обработката на информация и лични данни, които са на тяхно разположение, а също така и при употребата на определено оборудване за изпълнение на служебните им задължения.

2.2. Инструкцията се прилага при обработка на информация в рамките на всяка система или съхранявана на всякакъв носител, участващ в обработката на лични данни/информация в рамките на Дружеството, независимо от това дали обработката на лични данни/информация е свързана с вътрешни бизнес операции на Дружеството или с външни отношения на Дружеството с трети страни.

2.3. Инструкцията се прилага и по отношение на начина, по който Служителите на Дружеството използват оборудването и инструментите, с които разполагат за изпълнение на служебните им задължения.

2.4. Инструкцията може да се прилага във връзка с други политики, регулации, процедури и/или насоки, които с течение на времето са приети и въведени от Дружеството.

2.5. Всички въпроси, свързани със сигурността на информацията/личните данни, които не са обхванати от настоящата Инструкция, следва да бъдат насочвани към Управителя на Дружеството.

3. Класификация на информацията

3.1. Всяка/Всички информация/лични данни, която/които стане/-ат достъпна/-и за Служителите при изпълнение на служебните им задължения, ако са свързани с Дружеството и неговата дейност, клиенти или партньори за сътрудничество, се счита за собствена и поверителна информация на Дружеството, като по този начин се подчинява на защита в съответствие с приложимите закони и правната уредба относно защитата на поверителна информация, търговската тайна и личните данни.

3.2. За да се установи подходяща защита на информацията и личните данни, Дружеството извършва класификация на информацията в Дружеството. Информацията/личните данни подлежат на защита, независимо от това дали такава информация е на разположение на Служителя под формата на печатни материали, устройства за съхранение на данни, аудио/видео материали или по друг начин.

3.3. Обща класификация на информацията, приложима в рамките на Дружеството:

Категория	**Описание**	**Примери (включително, но неограничено до)**
Публична информация	Информация, която може да бъде обработвана и разпространявана в рамките на Дружеството или извън него без никакво отрицателно въздействие върху Дружеството, някой от неговите партньори, клиенти и/или свързани лица.	(а)Финансови отчети, публикувани до обществени органи; (б)Информация, достъпна чрез публични ресурси или публично известна по друг начин, освен ако не е станала обществено достояние вследствие на действия на Служители в нарушение на правилата за защита на информация/лични данни.
Вътрешна информация	Всяка употреба на информация по какъвто и да е начин, в случай, че е извършена в нарушение на изискванията на приложимите закони или подзаконови актове, тази Инструкция или всяка друга регулация, приета от Дружеството, може да навреди на интересите на Дружеството и/или неговите Служители, партньори и клиенти.	(а)Документи, разработени и/или изготвени от който и да е Служител на Дружеството; (б)Всички директории (информация за връзка и т.н.), установени и/или използвани за бизнес целите на Дружеството; (в)Всякакви вътрешни работни бележки, изявления, становища, разработени за бизнес нуждите на Дружеството или с цел ефективност на дейността на Дружеството;
Поверителна информация	Всяка информация от такова значение за Дружеството, който и да е от неговите клиенти и/или партньори или свързани лица, неоторизираното разкриване на която би могло да окаже неблагоприятно въздействие върху бизнеса, операциите, репутацията, цялостното състояние на Дружеството, неговите акционери, клиенти и партньори, като последица от такова разкриване, която би причинила сериозни вреди/щети на някое от тези лица.	(а)Политики, процедури, вътрешни правила, управленски решения; (б)Информация, за която е указано на Служителя, че е търговска тайна на Дружеството; (в)Друга информация от финансово, кадрово, правно, маркетингово естество, продажбени процедури, планове и операции; (г)Бизнес и продуктови планове; (д)Данни за лична идентификация; (е)Информация, която подлежи на защита по силата на споразумение за поверителност, което се подписва от всеки Служител; (ж)Информация, която подлежи на защита по силата на споразумения за поверителност или споразумения за сътрудничество, които Дружеството е сключило в хода на стопанската си дейност.

4. Системи, заети с обработка на лични данни/информация

4.1. Всякакви информационни системи, включително, но неограничено до компютърно оборудване, всякакъв тип софтуер, операционни системи, всякакви носители за съхранение, мрежови профили, електронни пощенски акаунти, системи за сърфиране и всяка друга техническа база и инструменти, използвани в дейността на Дружеството, се считат за собственост на Дружеството.

4.2. Всеки Служител следва да използва такова техническо оборудване и инструменти с дължимата грижа и внимание, и само за целите, свързани с дейността на Дружеството. Единственото изключение са случаите, когато Дружеството е предоставило на Служителя техническо оборудване (например мобилен телефон), което изрично позволява и личното му ползване.

5. Задължения на служителите

5.1. Цялата информация/Всички лични данни, която/които е/са на разположение на Служителя при изпълнение на служебните му задължения, се считат и се третират като поверителни, третирани като подлежащи на защита в съответствие с тази Инструкция и няма да се разкриват пред трети лица до или освен ако Ръководството обяви, че такава/-ива информация/лични данни е/са станало/-и публично достояние или по друг начин е прекласифицирана в информация, която вече не подлежи на защитата, установена с настоящата Инструкция.

5.2. Всички лични данни и друга информация, чрез която физическото лице може да бъде идентифицирано, се събират и обработват, само ако се изисква и до степента, необходима за изпълнение на служебните задължения на Служителя, при условие че тези дейности се извършват в рамките на правомощията, предоставени на Служителя и в съответствие със законовите изисквания за защита на личните данни (особено в съответствие с изискванията на Регламент (ЕС) № 2016/679 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)).

5.3. Всяко искане относно лични данни и/или обработка на лични данни, което Служителят при изпълнение на неговите/нейните служебни задължения е получил/-а от собствениците на данни - физически лица незабавно се препращат за по-нататъшна обработка до Ръководството.

5.4. Всеки Служител следва да се придържа към настоящата Инструкция, както и да спазва изискванията на приложимите закони и подзаконови актове, независимо дали са местни, регионални или международни, които установяват изисквания за обработка и защита на информацията/личните данни. Неспазването на Инструкцията се счита за съществено нарушение на установения трудов ред и би могло да доведе до дисциплинарни санкции или уволнение на Служителя по усмотрение на Дружеството. Това би могло да доведе и до административно-наказателна или наказателна отговорност на Служителя, действал в нарушение.

6. Управление на достъпа и защитата

6.1. Всички устройства, предоставени на Служителите, са достъпни за тях въз основа на техните служебни задължения, отговорности и принципа „необходимост да се знае". Достъпността до която и да е система не означава, че Служителят е оторизиран да преглежда или използва цялата информация в рамките на конкретната система.

6.2. Приложните потребителски идентификатори са уникални и идентифицират конкретен Служител. Всеки Служител е отговорен за всички действия, свързани с неговия/нейния личен идентификационен профил, поради което основното задължение е да се гарантира, че идентификацията на Служителя не е на разположение на трети лица и дори на други Служители, освен ако Дружеството е установило различен от този ред.

6.3. Паролите за сигурност на системата се създават с дължимата грижа, при условие че не са лесни за отгатване, не включват лични данни, се променят редовно (не по-малко от веднъж на 6 месеца). Всеки Служител е лично отговорен/-а за съобразяването на паролата за сигурност с тази Инструкция и всички други правила на Дружеството.

6.4. Служителят осъществява достъп до поверителна/-и информация/лични данни само ако такова правомощие е предоставено на Служителя с неговия/нейния Трудов договор и/или изрично упълномощаване на Служителя от страна на Дружеството.

7. Мерки за сигурност

7.1. Всички лични данни и информация, събрани и обработвани под каквато и да е форма (на хартия, електронна и др.), се подчиняват на изискванията на настоящата Инструкция и всяка нормативна уредба по отношение на събирането, обработването, защитата и задържането на информацията/личните данни, а съответните документи се съхраняват на безопасно място, определено от Дружеството за период на задържане, предвиден от приложимите закони и/или посочен от Дружеството.

7.2. Служителите нямат право да съхраняват никаква поверителна информация на своите устройства, с изключение на информацията, която временно е необходима за конкретна, свързана с работата, дейност. Цялата поверителна информация и информацията, необходима за лична идентификация, следва да се съхранява само в режим на облачно съхранение, одобрен от ИТ персонала на Дружеството, и на интранета на Дружеството. Всяко изтегляне на такива файлове на местни устройства следва да се избягва и да се ограничава само до необходимост, свързана с обработката на информацията за целите на работата.

7.3. Достъпът до Интернет и операциите, извършвани от Служителите там съгласно изискванията на приложимите закони и подзаконови актове, могат да бъдат филтрирани и наблюдавани от надлежно упълномощен персонал на Дружеството.

7.4. Всички мобилни преносими устройства (включително лаптопи, таблети, смартфони и други ръчни изчислителни устройства), както и всички облачни места за съхранение на информация, следва да бъдат надлежно обезопасени, за да се предотврати неоторизиран достъп.

7.5. Само системите и програмният софтуер, лицензирани и оторизирани от Дружеството, могат да бъдат инсталирани и използвани на оборудване и инструменти, използвани в Дружеството. Преди изтегляне или инсталиране на софтуер на устройства, в притежание на и използвани от Служители за целите, описани в настоящата Инструкция, трябва да се получи разрешение.

7.6. В случаите, когато Служителите използват домашни устройства за достъп до корпоративни ресурси на Дружеството (напр. CRM система за управление на взаимоотношенията с клиентите, електронна поща, онлайн/облачни бази данни), Служителите са длъжни да спазват изискванията на настоящата Инструкция така, както биха използвали оборудване, предоставено им от Дружеството. Съответно, забранява се съхраняването на лични данни и информация, свързани с Дружеството на съответното устройство; всяка обработка на личните данни се разрешава само чрез облачни и онлайн места за съхранение, използвани от Дружеството.

7.7. Строго се забранява използването на обществени устройства за достъп (напр. в интернет кафенета, библиотеки и т.н.), освен ако не се касае за случай на критична и спешна необходимост, свързана с работата и Прекият ръководител на Служителя е предоставил изричното си писмено съгласие за това действие.

7.8. В случай, че на Служителя бъде предоставен достъп до система за съхранение на файлове на клиент или партньор за сътрудничество на Дружеството, Служителят е длъжен да използва предоставените от клиента или партньора инструменти за достъп и да спазва предоставените указания за изискванията за сигурна обработка на информация/лични данни (включително използване на системи за криптиране, пароли, ограничения при използването на данни, използване на специализирани местоположения и т.н.).

7.9. От момента, в който по преценка на Дружеството информацията/личните данни, подлежащи на защита, вече не са необходими за дейността на Дружеството, тази/тези информация/лични данни се заличават, всички техни копия се унищожават и Служителите, участващи в обработката на съответната/-ите информация/лични данни, се уведомяват съответно за задължението си да унищожат и върнат на Дружеството информацията/личните данни, които вече не се необходими за изпълнение на служебните им задължения, и по-специално да върнат обратно на Дружеството, да изтрият и да унищожат копията в случай на прекратяване на трудовото правоотношение на съответния Служител.

7.10. Никаква/-ви информация/лични данни, посочени в настоящата Инструкция, няма да се изпращат, препращат или по друг начин предоставят на Трета страна, освен ако това не е необходимо за изпълнение на служебните задължения на Служителя и до степента, която е необходима за изпълнението на тези задължения. В случай на предаване и предаване на лични данни на Трети страни, се гарантира, че личните данни са защитени и са взети съответните мерки за сигурност.

7.11. Дружеството одитира системите, използвани при обработката на информация/лични данни, за да контролира непрекъснатото спазване на настоящата Инструкция и приложимите законови изисквания.

8. Забранени дейности

8.1. С изключение на специфично установените изключения, в никакъв случай и при никакви обстоятелства не трябва да се използва оборудване, системи или инструменти, собственост на Дружеството, нейните клиенти или партньори за сътрудничество, за цели, които не са свързани с трудовите задължения на Служителя, или които не са свързани със стопанската дейност на Дружеството.

8.2. Следващите дейности са строго забранени, без изключения:

(а) Нарушаване на правата на което и да е лице или дружество, защитени от права на интелектуалната собственост, включително, но не само, инсталиране, копиране, разпространение или съхранение на системите или оборудването на Дружеството на незаконни софтуерни продукти, онлайн платформи и всяко друго електронно съдържание, нелицензирано за използване от Дружеството;

(б) Неразрешено копиране на материали, обект на авторско право;

(в) Нарушаване на правата на което и да е лице чрез прекомерно и ненужно събиране и обработка на личните данни на такова лице;

(г) Достъп до лични данни, сървър или профил с цел, различна от извършване на търговска дейност на Дружеството или изпълнението на служебни задължения на конкретния Служител;

(д) Изнасяне на софтуер, техническа информация, софтуер или технология за криптиране в нарушение на приложимите международни или национални закони и нормативни актове и/или указания на Дружеството;

(е) Изнасяне на всякакви лични данни или информация, които са собственост на Дружеството или са поверителни за него, ако такова изнасяне не се изисква в хода на стопанската дейност на Дружеството или при изпълнение на служебните задължения на Служителя и/или е в нарушение на вътрешните правила на Дружеството, приложимите закони или подзаконови актове;

(ж) Разкриване на паролата за профила на Служителя на други лица и разрешаване на използването на такъв профил от други лица (включително, но не само членове на семействата на Служителите);

(з) Предоставяне на измамни оферти за продукти, артикули или услуги, произхождащи от профила на Дружеството;

(и) Нарушения на сигурността или прекъсвания на мрежовата комуникация. Такива нарушения на сигурността включват, но не се ограничават до достъп до лични данни, на които Служителят не е определен като получател или не се логва в сървър или профил, до който Служителят не е изрично упълномощен за достъп, освен ако такива права на достъп не се предоставят на Служителя поради участието му/ѝ в конкретен проект на Дружеството;

(й) Използване на всяка програма/скрипт/команда или изпращане на съобщение от всякакъв вид с намерението да се окаже влияние на или да се прекрати потребителската сесия по какъвто и да е начин.

9. Докладване на инциденти по сигурността

9.1. Всички инциденти по сигурността или обработването на информация/лични данни или заплахи от инциденти незабавно се съобщават на Ръководството, което съответно предприема всички мерки за предотвратяване на евентуални вреди/щети, отстраняване на причинените вреди/щети и възстановяване на предходния безопасен статус.

9.2. Ръководството има задължението да осигури по-нататъшното отчитане на нарушаването на сигурността на информацията/личните данни пред съответните органи и физически лица, както и когато това е предвидено в приложимите закони и подзаконови актове и/или законите на Европейския съюз.

_____

подпис

_____

[Име, Фамилия, длъжност на подписващия]