Версия:	1.0
Дата на версията:	19.10.2023 г.
В сила от:	19.10.2023 г.
Изготвени от:	АйТи Бейслайн ООД, консултант
Одобрени от:	Проф. д-р Димитър Димитров, ректор на УНСС
Ниво на поверителност:	Ниво 2 – Служебно ползване

Контроли за сигурност на човешките ресурси

СЪГЛАСНО ISO/IEC 27001:2022

РЕГИСТРИРАНЕ НА ИЗМЕНЕНИЯТА	
Стр.	Същност на изменението

CONTENTS

1. ЦЕЛ

- Настоящата процедура определя реда, отговорностите, както и системата от мерки, способи и средства при внедряване и прилагане на механизми за контрол по отношение сигурността на човешките ресурси в организацията;
- Осигуряване на подходящо ниво на защита, надеждно управление и ефективен контрол на активите и ресурсите на организацията;
- Недопускане или намаляване до минимум на щетите от произшествия, свързани с контрола на процесите по управление на активите и ресурсите.

2. ОБХВАТ

Настоящия документ обхваща процесите по избор, внедряване, прилагане и мониториране на механизми за контрол по отношение сигурността на човешките ресурси, съгласно клауза 6 на Приложение А от ISO27001: 2022.

3. ОТГОВОРНОСТИ

Настоящата процедура обхваща всички йерархични нива и служители на организацията. Пряка отговорност за прилагане и спазване на настоящата процедура носят лицата от организацията, както следва:

- **Ректор/Представител на ръководството** за непрекъснат контрол на процесите и осигуряване на необходимите ресурси;
- **Мениджър ИТ Сигурност** и **Мениджър ИТ** за оказване на контрол и методическа помощ в структурните звена и пряко управление на процесите в техните правомощия и функционални задължения;
- **Мениджър СУИС** за координация и правилно управление на процесите и дейностите, както и документирането им;
- **Директор Дирекция Човешки ресурси** за прилагане на Процедурата и усъвършенстването на СУИС.
- **Служителите от организацията** за прилагане на Процедурата и усъвършенстването на СУИС.

4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

Не се въвеждат нови термини и съкращения.

5. ДЕЙСТВИЯ И МЕТОДИ

Изборът на механизми за контрол по отношение сигурността на човешките ресурси е съгласно клауза 6 на Приложение А от ISO27001: 2022.Внедряването им се извършва като се вземат предвид правни, законови, регулаторни, договорни и други изисквания с цел постигане високо ниво на информационна сигурност в организацията, както и съответствие на СУИС с изискванията на стандарта.

А. 6.1. ПОДБОР НА КАДРИ/СКРИНИНГ

Механизъм за контрол: *Трябва да бъдат извършвани проверки за верификация на биографичните данни на всички кандидати за работа, преди да се присъединят към организацията и текущо, в съответствие със приложимите закони, разпоредби и етика, и съгласно изискванията на бизнеса, класификацията на информацията, до която имат достъп, и поеманите рискове.*

Преди да назначи на работа одобрените за съответната позиция кандидати Организацията изисква набор от документи, удостоверяващи идентичността им, както и доказателства за тяхното професионално, квалификационно, трудово, здравословно, съдебно и друго състояние. Събират се данни, пропорционални на бизнес изискванията и потенциалните рискове за длъжността, както и съобразно класификацията на информацията, до която ще се осъществява достъп от лицето.

Това са средства за контрол като:

- наличност на препоръка за лицето – при необходимост и решение на Ръководството за определени длъжности;
- проверка (за пълнота и точност) на биографията на кандидата;
- потвърждение на декларираните образователни и професионални квалификации;
- проверка на самоличността (паспорт, лична карта или подобен документ);
- други.

Директор дирекция „Човешки ресурси“ чрез началник отдел „Управление на човешките ресурси“ извършва предварителен контрол за законосъобразност на процеса по постъпване на служители на работа в УНСС. Началник отдел „Управление на човешките ресурси“ попълва лист за извършване на предварителен контрол за законосъобразност на процеса по назначаване на служители по трудови правоотношения в УНСС и поделения, в който следи за:

- Отговаря ли кандидатът на изискванията за длъжността, на която се назначава;
- Спазени ли са изискванията на вътрешните процедури и други нормативни изисквания, свързани с постъпването на работа.
- Съответства ли назначението с утвърденото щатно разписание;
- Налице ли е вакантна длъжност и други.

В случаите когато при първоначалното назначаване или при повишение, длъжността на лицето включва то да има достъп до средства за обработване на информация и в частност, ако се обработва поверителна информация, например финансова такава или строго поверителна информация, организацията преценява и по възможност прилага и допълнителни, по-подробни верификации.

В ситуации, при които проверката не може да бъде завършена навреме до момента за назначаване на лицето, се прибягва до смекчаващи механизми за контрол, докато прегледът не приключи, например:

- забавено въвеждане в длъжност;
- забавено внедряване на корпоративните активи;
- въвеждане в работата с ограничен достъп;
- прекратяване на трудовото правоотношение, при необходимост.

На работа в организацията се назначават предимно лица, притежаващи необходимата компетентност, знания и практически умения за съответната длъжност. Допуска се и наемането на служители, непритежаващи необходимия опит, като в последствие се предвижда осигуряване на вътрешно и/или външно обучение, с изключение на позиции, чиито компетенции са определени от нормативни изисквания.

В зависимост от критичността на ролята на даден служител, проверките би трябвало да се повтарят периодично, за да се потвърди текущата пригодност на лицето.

Преките ръководители контролират подчинения им персонал. Особено внимание се обръща на потенциални или вече възникнали лични или финансови проблеми, изменения в поведението или в начина на живот, повтарящи се отсъствия и доказателства за стрес или депресия, които могат да доведат до измама, кражба, грешки, податливост към финансови облаги, корупция или други усложнения, кореспондиращи със сигурността.

Информацията за всички кандидатствали за позиции в организацията се събира и обработва в съответствие с приложимото законодателство, като се съблюдава защитата на личните данни (съобразно ЗЗЛД), защитата на личната тайна (касаеща здравословния статус на кандидата), трудовото законодателство и др.

А. 6.2. СРОКОВЕ И УСЛОВИЯ ЗА НАЕМАНЕ НА РАБОТА

Механизъм за контрол: *В договорните задължения на служителите и доставчиците трябва да бъде включен техния ангажимент и ангажимента на организацията по отношение на информационната сигурност.*

Сроковете и условията за наемане на работа се регламентират в процедурите и договорите.

При управление на процеса организацията контролира следния регламент:

- Ролите и отговорностите във връзка с ИС се комуникират с кандидатите по време на процеса, преди назначаването на работа;
- В договорните задължения на лицето Организацията залага регламент за съгласие на персонала с правилата и условията, свързани със сигурността на информацията. По-конкретно в Правилника за вътрешния трудов ред в раздел Задължения в т. 41 е посочено, че: „Да не разгласяват информация, сведения и факти, съставляващи служебна информация и станала им известна при и по повод изпълнението на служебните им задължения и две години след прекратяването на трудовия им договор“.
- Всички служители, подписват „**Декларация за „Конфиденциалност**“, като част от договорът им за постъпване на работа преди да получат достъп до средствата за обработка на информация на организацията; третите страни подписват Споразумение за поверителност/конфиденциалност с трети страни. При изрично изискване от страна на клиент служителите на организацията подписват Декларация за конфиденциалност, във връзка с информацията, собственост на клиента, до която ще имат достъп по време на работата си с него. Тези споразумения се преглеждат при изменение на условията на назначението или на договора, особено когато служителите напуснат организацията, или когато изтичат договорите им.

Където е приложимо, се залага като условие на споразумението ангажиментите, поети в него, да продължат за определен период след прекратяване на договорните отношения;

- служителите, доставчиците и другите потребители съзнават своите отговорности по отношение класифицирането на информацията и управлението на информационните активи (свързани с информационните системи и услуги);
- отговорностите на служителя, доставчика или потребителя от трета страна за управление на информация, която е получена от други (външни или трети) страни;
- отговорностите на Организацията по управление на личната информация, включително и тази лична информация, която е получена в резултат на или в течение на работата;
- действията, които се предприемат в случаите, когато служителят, доставчикът или потребителят от трета страна пренебрегва изискванията за сигурност на Организацията.

А. 6.3. ОСЪЗНАВАНЕ, ОБУЧЕНИЕ И ПРАКТИЧЕСКА ПОДГОТОВКА В ОБЛАСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Механизъм за контрол: *Всички служители на организацията и където е уместно, доставчиците трябва да получат подходящо обучение за осведомяване и редовно актуализиране на знанията по политиката по информационна сигурност на организацията и специфичните политики, в съответствие с техните работни функции.*

Дейностите за осъзнаване на сигурността на информацията от страна на служителите са предвидени в съответствие с Политиката за информационна сигурност на организацията, специфичните политики и съответно приетите процедури. Те се провеждат планирано, като се вземат предвид и ролите на служителите в организацията, както и очакванията на самата организация за нивото на тяхната осъзнатост.

Обучението и осведомяването на служителите по аспектите на сигурността започва с процес на формално въвеждане, предназначен да запознае новоназначения персонал с политиките, изискванията и очакванията за сигурност на организацията, преди да бъде даден достъп до информация или услуги. По периодиката на своето провеждане обученията биват: първоначално /встъпително/ и текущо. Обучението за повишаване на осведомеността позволява на служителите на организацията да разпознават проблемите и инцидентите със сигурността и да действат, съгласно установената практика и персонална роля. Прекият ръководител/Директор дирекция ЧР предоставя на новопостъпилия служител съответните документи за конкретната позиция, нормативна, техническа литература и документите на ИС, пряко касаещи дейността.

Организират се вътрешни и/или външни обучения, като всички те се документират и се съхраняват, както следва:

- за общите/груповите обучения доказателства като програма, протокол от провеждане и др. се съхранява от Мениджър СУИС;
- копията от протоколи и сертификати от индивидуалните обучения се прилагат в личното досие на служителя и се съхраняват от Директор дирекция ЧР.

С вътрешното обучение, свързано с внедряването, поддържането и усъвършенстването на ИС се цели персоналът на организацията да се запознае подробно с политиката и целите по сигурността на организацията и с изискванията на регламентите на стандарта ISO 27001:2022.

С външното обучение се цели обучаващият се персонал да получи компетентни знания от оторизирани организации по въпроси, свързани с дейността на организацията и усъвършенстване на сигурността.

Външно обучение се провежда в следните случаи:

- усвояване на действащи или нови стандарти;
- усвояване на даден продукт;
- усвояване на даден процес;
- за обучение на вътрешни и водещи одитори ;
- за усъвършенстване на знанията и уменията по сигурността;
- при внедряване и усвояване на нови технологии и направления, касаещи информационната сигурност;
- за изучаване на международния опит по аспектите на сигурността и други.

По преценка на Ръководството на организацията, Мениджър СУИС и/или Директор дирекция ЧР извършват подходящи инструктажи във формата на обучения на доставчици и потребители от трета страна в съответствие с техните функции на работа.

За планираните обучения организацията поддържа документ Годишен план на обученията на служителите. Процесът по изготвяне на плана включва:

1. През годината, предхождаща годината на реализиране на обучението, всеки ръководител на структурна единица предава планът за обучение на управляваната от него структурна единица на директора на дирекция „Човешки ресурси”, а той от своя страна на началник отдел “Управление на човешките ресурси”.

2. Началник отдел "Управление на човешките ресурси", обобщава всички планове за обучение на структурните единици в "Годишен план за обучение на служителите в УНСС".

3. Изготвеният Годишен план се внася за утвърждаване от Ректора от директора на дирекция "Човешки ресурси".

Организиране и провеждане на обучение по Годишен план за обучение в УНСС .

1. През годината на осъществяване на обучението се реализират само курсове на обучение на непреподавателския състав на УНСС.

2. В срок минимум до 10 дни преди началната дата на осъществяване на курс /семинар/ за обучение, ръководителят на основното звено подава в отдел "Управление на човешките ресурси" съответна заявка за провеждане на обучението.

3. От своя страна, след като е получил заявката, началник отдел "Управление на човешките ресурси" попълва Финансово предложение с размера на финансовите средства, съблюдавайки прецизното и целесъобразно разходване на финансовите средства в рамките на утвърдения бюджет на УНСС.

4. Курс на обучение се провежда след като заявката за обучение и финансовото предложение са приемат от директора на дирекция "Човешки ресурси" и се утвърждава от Ректора на УНСС.

5. В срок до 10 дни след реализиране на семинар, ръководителите на основните звена, чиито подчинени служители са преминали курс на обучение, представят в доклад до директора на дирекция "Човешки ресурси" отчет.

6. Въз основа на информацията по т. 5., началник отдел "Управление на човешките ресурси" отразява настъпилите промени по обучението на непреподавателския персонал в Годишния план за обучение, всяко тримесечие под формата на "Актуализация на годишен план".

При необходимост от провеждане на непланирано обучение Служителят подава към прекия си ръководител заявка за одобрение по e-mail. Заявката е в свободен текст и най-общо съдържа: име и длъжност на служителя, обучение, в което желае да се включи, обосновка за необходимостта от провеждане. По възможност може да се допълни и информация за организацията, която го организира, лекторите, стойността и др. Одобрение или отхвърляне на заявката прекия ръководител връща на заявилия служител като отговор на e-mail.

А. 6.4. ДИСЦИПЛИНАРЕН ПРОЦЕС

Механизъм за контрол: *В организацията трябва да има внедрен и комуникиран дисциплинарен процес, за служители и други съответни заинтересовани страни, извършили нарушение на политиката за сигурност на информацията.*

При регистриране на обективни доказателства или потвърдена информация за пробив в сигурността, Ръководството на организацията управлява дисциплинарен процес.

Дисциплинарният процес осигурява законово, коректно и обективно отношение към служителите, за които се предполага, че са виновни за случването на подобни събития. При управление на дисциплинарния процес се осигурява незабавна реакция, като се отчитат фактори като:

- естеството и тежестта на пробива и неговото влияние върху процесите и продуктите на организацията;
- дали това е първи случай или поредица от нарушения;
- дали нарушителят е бил правилно обучен;
- нормативната база;
- договорните отношения и др.

При констатиране на сериозни нарушения и престъпления, дисциплинарният процес включва незабавни действия по отменяне на задължения, права на достъп и привилегии и незабавно извеждане на нарушителя вън от обекта на организацията, ако е необходимо такова действие.

Прилагането на дисциплинарният процес в Организацията е част от превенцията за предотвратяване на нарушения на политиките и процедурите по сигурността и всякакви други пробиви (сривове) в сигурността от страна на служителите, доставчиците и потребителите от трета страна.

При налагане на дисциплинарни мерки към служителите на организацията се прилагат регламентите на Кодекса на труда, а при някои случаи се преминава по реда на подвеждане към съдебна отговорност. При нарушения от страна на трети страни и доставчици се прилагат регламентите, разписани в договорите и/или подвеждане под съдебна отговорност.

А. 6.5. ПРЕКРАТЯВАНЕ ИЛИ ПРОМЯНА НА ОТГОВОРНОСТИ НА СЛУЖИТЕЛИ

Механизъм за контрол: *Отговорностите и задълженията по информационна сигурност на служители или доставчици, които се запазват след прекратяване или промяна на службата, трябва да бъдат ясно определени, комуникирани и възложени.*

Организацията е регламентирала процеса като гарантира, че напускането от страна на служител, доставчик или потребител от трета страна се управлява и контролира по начин и с механизми, които изключват възможността от нарушаване характеристиките на активите (конфиденциалност, цялостност и наличност).

Регламентът за отговорностите при прекратяване на служебните ангажименти на дадено лице включва:

- нормите за поведение на съответния служител (в аспектите на сигурността);
- изискванията на законите и друга нормативна база;
- служебните ангажименти по отношение на сигурността;
- изискванията на Споразумение за поверителност/конфиденциалност с трети страни и/или клауза „Конфиденциалност“ като част от договорът за постъпване на работа;
- сроковете и условията за изпълнение на служебните ангажименти на съответния служител, доставчик или потребител от трета страна.

Отговорностите и задълженията, които все още са в сила след прекратяване на наемането на работа се регламентират в договорите със служителя, доставчика или потребителя от трета страна.

Измененията в отговорностите или служебните ангажименти се управляват по начин, който позволява, процесът на прекратяване на съответната отговорност или служебни ангажименти да бъдат контролирани. При преназначаване промените в отговорностите във връзка с ИС се управляват като се прекратява текущата отговорност, а в последствие се възлага новата такава, която е присъща на променената длъжност.

Този процес се управлява от Директор дирекция “Човешки ресурси”. В случай на доставчик или потребител от трета страна, този процес на прекратяване на отговорността се извършва от Ръководството с непосредствените действия на Мениджър СУИС и Директор дирекция “Човешки ресурси”.

Когато се налага със Заповед на Ръководството, Организацията може да внесе изменения в споразуменията за поверителност с персонала и работните споразумения със служителите, доставчиците, клиентите или потребителите от трета страна. В тези случаи Организацията писмено уведомява всички заинтересовани лица за настъпилите изменения и основанието, което ги налага.

Процесът по напускане, преместване или уволнение на персонал се стартира чрез писмена Заповед, с която лицето се уведомява за промяната. Преди напускане, уволненият служител предава всички:

- пароли за достъп до информационни системи на Организацията;
- всички активи на Организацията, които са се намирали до момента на уволнението под негово управление и собственост.

Документът за зачисляване/връщане на зачислените активи се подписва от уволнения/напускащия служител и един от: Директор дирекция “Човешки ресурси”, Мениджър СУИС или Мениджър ИТ сигурност.

Уволненият/напусналият служител се инструктира да спазва клаузите за поверителност, залегнали в неговия договор и Декларация/Споразумение за поверителност/конфиденциалност, ако има такива.

В Протокола за връщане на материални активи, (преди подписите “предал” и “приел”) се отбелязва, че уволненият служител е инструктиран за спазване изискванията за поверителност.

В случай, че уволненият служител откаже да подпише Протокола връщане на материални активи, същият се подписва от длъжностно лице на Организацията, което се явява в качеството на свидетел за върнатите активи.

А. 6.6. КОНФИДЕНЦИАЛНОСТ И НЕИЗПЪЛНЕНИЕ НА ДОГОВОРЕНИ ЗАДЪЛЖЕНИЯ

Механизъм за контрол: *Споразуменията за поверителност или неразкриване, отразяващи нуждите на организацията за защита на информацията, трябва да бъдат идентифицирани, документирани, редовно преглеждани и подписани от персонала и други съответни заинтересовани страни.*

Споразуменията за конфиденциалност и лоялност касаят изискванията за защита на класифицираната информация в организацията, като се прилагат за нормативно определени срокове.

При изготвяне на споразуменията за конфиденциалност Ръководството определя:

- информацията, която трябва да бъде защитена;
- отговорностите, касаещи периода след приключване на споразумението;
- отговорностите и действията на подписващите, за да се избегне неразрешено разкриване на информация (да се прилага принципа “необходимо е да се знае”);
- собствеността върху информацията и интелектуалната собственост;
- разрешеното използване на информация и правата на декларатора да използва информацията;

- процес за уведомяване и докладване за неразрешено разкриване или нарушаване на поверителността на информацията;
- сроковете, в които информацията трябва да бъде защитена, върната или унищожена, ако е възможно при прекратяване на споразумението;

Анализирайки конкретните изисквания за сигурност, организацията може да включи други елементи в споразумението, които счита, че са необходими за защита на информацията.

Споразуменията за конфиденциалност защитават организацията и информират подписващите за техните отговорности, като по този начин се защитава, използва и разкрива информация по отговорен, контролиран и санкциониран начин.

За различни обстоятелства Организацията може да използва различни форми на Споразумения за поверителност/конфиденциалност.

А. 6.7. РАБОТА ОТ РАЗСТОЯНИЕ

Механизъм за контрол: *Трябва да бъдат внедрени политика и мерки по сигурността при работа от разстояние, за да се защити информацията, която е достъпна, обработена или съхранявана извън помещенията на организацията.*

Политиката за работа от разстояние има за цел да защити данните на УНСС, които се достъпват отдалечено, както и преноса, обработката и съхраняването им в и до отдалеченото мобилно устройство.

Прилагат се следните мерки за защита и механизми за контрол:

- Устройствата, с които ще се осъществява отдалечен достъп до информация или ресурси на УНСС, задължително трябва да са осигурени с продукти за защита от злонамерен софтуер, и с включена защитна стена.;
- Достъпът се осъществява само през SSL VPN с подходящи шифроващи алгоритми, освен в случаите, когато се достъпва публична услуга на УНСС;
- Устройствата са персонализирани с наложени съответните политики за сигурност. Там, където е невъзможно да се наложат политики з сигурност /Linux Workstations, MacOS и лични устройства/, се лимитират достъпите до възможния минимум за постигане на целите на работата;
- Достъпа до имейл комуникацията и пространството за съхранение на файлове, които са облачна услуга, е осигурен с двуфакторна автентикация;
- Достъпа до данните, в зависимост от тяхното ниво на чувствителност, се определя от привилегиите за достъп до информация за конкретния потребител или група от потребители;
- Служителите имат задължението да заключват екрана на работните станции при временно прекъсване на работата с тях, дори когато са под наблюдението им, с цел предотвратяване на неоторизиран достъп до информацията от лица в същото помещение.

А. 6.8. ДОКЛАДВАНЕ НА СЪБИТИЯ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Механизъм за контрол: *Организацията трябва да осигури за персонала механизъм за своевременно докладване на наблюдавани или предполагаеми събития за сигурност на информацията чрез подходящи канали.*

Указанията за докладване при инцидент включват:

Когато служител забележи аномалия или отклонение в очакваното /нормално/ поведение на информационна система, следва да уведоми по установен канал Дирекция ИТ, а ако това е невъзможно, чрез уведомяване на прекия си ръководител устно или чрез телефонно обаждане. В тези случаи преките ръководители имат задължението да докладват това събитие по приетия официален канал.

Важно е да се докладва всяко съмнение за срив (или пробив в сигурността), дори в последствие да се установи, че то е по причина, различна от инцидент със сигурността.

Не се допуска обсъждането инцидент с трети лица, без изричното разрешение на Мениджър ИТ Сигурност.

Инцидент е непредвидимо или трудно прогнозируемо събитие/явление или действие с висока интензивност - бедствие, авария, катастрофа, отказ на функционалност на система, стоп на бизнес процеси и други, чието осъществяване представлява източник на изключителна непосредствена заплаха за информационните активи: живота, здравето, имуществото на групи от хора, за унищожаването на съществени информационни, материални, финансови и други ресурси и за функционирането на организацията.

Организацията е приела следните типове инциденти:

- загуба на услуга, устройство или средства;

- неправилно функциониране на системата или претоварвания на системата;
- човешки грешки;
- несъобразяване с политиките или указанията;
- нарушения на мерките за физическа сигурност;
- неконтролирани изменения на системата;
- неправилно функциониране на софтуера или хардуера;
- нарушения на достъпа.

Проблем представлява основната причина за един или няколко инциденти/значими инциденти.

Инциденти или други потенциално значими събития, имащи отношение към информационната сигурност, се приемат и от трети страни и лица, независимо дали организацията има договорни взаимоотношения с тях. Независимо от вида и формата на докладване, организацията следва да може да проследи историята на всяко събитие чрез генерираните по повода записи. Приемат се комуникация по ел. поща, използване на тикет системи (собствена или на доставчик), хартиени документи, видеозаписи или друго, подходящо за целта. Независимо от вида и източника на докладваното, последващите действия следва да са в унисон с приетите процедури.

При констатиране на слабости в сигурността, които могат да доведат до инцидент, свързан със сигурността, се докладва незабавно, съгласно правилата в предходната точка.

Трети страни, с които организацията има договорни взаимоотношения по повод управлението на информационната сигурност, могат да докладват потенциални слабости по начин, по който те преценят (относимо за трети страни) или според регламентираната форма на докладване (за страни в договорни взаимоотношения). Независимо от вида и източника на докладваното, последващите действия следва да са в унисон с приетите процедури.

При инцидент с мрежовата и информационната сигурност Мениджър ИТ сигурност уведомява съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност. За уведомяването се използва формата, посочена в Приложение № 7 към чл. 31, ал. 2 от НМИМИС.

6. СПРАВОЧНИ ДОКУМЕНТИ

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022

7. ПРИЛОЖЕНИЯ

Годишен план на обученията
Декларация конфиденциалност
Споразумение конфиденциалност с трети страни

Дата: 19.10.2023 г.

Утвърдил: ……
Ректор: Проф. д-р Димитър Димитров

ПРИЛОЖЕНИЯ:

Годишен план на обученията за **…… г**

Тема на обучение	Причини за провеждане на обучението	Цел на обучението	Участници в обучението (брой и длъжност)	Провеждащ обучението (вътрешно/ външно)	Отговорници за провеждане на обучението	Планирани средства за обучение

Общо планирани средства:

Ръководител на основното звено: .....
(подпис)

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ

Долуподписаният/ата .....
Структурно звено……
Длъжност……..

Декларирам, че:

- Се задължавам да не разгласявам по какъвто и да било начин и под каквато и да било форма Конфиденциална информация, станала ми известна по време и по повод връзка работата ми, отнасяща се до дейността и интересите на УНСС. Потвърждавам също, че няма да разпространявам и научена от мен информация от личен характер за служители на организацията.
- Приемам да се отнасям грижливо към документацията/информацията, с която работя при изпълнение на служебните си задължения и да не показвам, разкривам или разгласявам нейния вид или съдържание на други лица, освен на упълномощените представители на УНСС, чиято собственост се явяват документите/информацията.
- Конфиденциална информация по смисъла на настоящата Декларация означава данни и информация от интелектуално, техническо, научно, стопанско или търговско естество, които УНСС и/или дружества от неговата група законно притежават и/или имат законови или договорни задължения да пазят. В частност, Конфиденциална информация означава данни и информация, включително, но не само, финансови прогнози, финансови, технически и търговски условия, бизнес планове и свързана техническа, търговска или бизнес документация, бизнес и ценови политики и практики, оферти, системи за изчисляване на разходите, процедури за таксуване и събиране, дейности за развитие на бизнеса и планове за съществуващите и бъдещи бизнес направления, продукти и услуги, информация относно продажбите, обема на продажбите, методите за продажби и маркетинг, финансови резултати, предложения за продажба, самоличност на клиенти, видове клиентски покупки, източници на доставка, списъци с клиенти, доставчици и партньори, бизнес прогнози, продажби и мърчандайзинг, идентичността и естеството и условията на бизнес отношения с доставчици, заемодатели, независими изпълнители и служители, патенти, патентни заявки, компютърни обекти или програмен код, изследвания, изобретения, процеси, проекти, формули, техники, чертежи, концепции, снимки, записи, инженерство, компютърен софтуер и всички писмени материали, отнасящи се до такъв софтуер, спецификации, математически данни и изчисления

относно игри, стандарти, ръководства, наръчници, прототипи, изобретения, бази данни, информация за хардуерна конфигурация, системи, методи, програмни материали, процеси, нови и разработващи се продукти и услуги, маркетингови данни, планове и концепции, ноу-хау, подобрения, изследователски проекти, открития, разработки, лични данни, както и всякакви други данни под каквато и да е форма и съдържание, които се съхраняват на какъвто и да е носител и са свързани с която и да е от дейностите на УНСС или нейни свързани лица, както и всякакви други данни, които едностранно са определени като поверителни от „УНСС. За избягване на всякакво съмнение, липсата на маркиране или обозначаване на информация като „конфиденциална“ няма да попречи информацията, която е била или ще бъде достъпна от или разкрита, да се счита за Конфиденциална информация съгласно настоящата Декларация.

- Разкриване, предоставяне и/или разпространение на Конфиденциална информация по смисъла на настоящата Декларация представлява всякакъв вид устно или писмено изявление, предаване на информация на хартиен, електронен или друг носител, включително по поща, факс, електронна поща, както и всякакъв друг начин на разкриване на информация на трето лице, в това число чрез средствата за масово осведомяване, печатните издания или интернет.
- Задължението ми за неразкриване на Конфиденциална информация е безсрочно.
- Задължавам се да пазя Конфиденциалната информация добросъвестно и да не я разпространявам пред трети лица.
- Задължението за неразкриване на Конфиденциална информация няма да се прилага по отношение на информация, която е била публично оповестена или разкрита от УНСС.
- След приключването на трудово правните ми отношения (поради причини от всякакъв характер) и при поискване по всяко друго време, аз се задължавам незабавно да върна всички документи и техни копия, извадки или записи от тези документи, бележки, меморандуми, фотографии, скици, звукови или видео записи, пароли за достъп или други материали, изготвени от мен или предназначени за мен във връзка с работата ми, свързани с дейността на УНСС, с нейни служители или контрагенти.
- Осъзнавам, че всяка техническа и бизнес информация на организацията и клиентите й, която е конфиденциална, представлява търговска тайна и е чужда собственост. В случай че бъда задължен/а от съдебните власти да предоставя такава информация, ще предоставя на “УНСС копия от всички предоставени от мен сведения.

Дата: _____ г. Декларатор: _____

имена, подпис

СПОРАЗУМЕНИЕ ЗА ПОВЕРИТЕЛНОСТ/КОНФИДЕНЦИАЛНОСТ С ТРЕТИ СТРАНИ

Подписаният/та ....., ЕГН ....., притежаващ/а лична карта № ....., издадена на ..... г. от МВР ....., в качеството ми на ..... от..... ,

ДЕКЛАРИРАМ:

1. Запознат съм със съдържанието на фактите, сведенията и предметите на Организацията, които са категоризирани като класифицирана информация, и не подлежат на публично огласяване.

2. При осигурен законен достъп до лични данни или друга служебна информация се задължавам да управлявам тази информация, съобразно изискванията на ЗДОИ, ЗЗЛД, ППЗЗЛД и другата нормативна база.

3. При регистриране на опит или при заплаха от инцидент, засягащ информационната сигурност на Организацията, се задължавам да уведомя незабавно Ръководството.

4. Задължавам се да не разпространявам факти, сведения и предмети, които са получени по повод изпълнението на договорените дейности, през целия период на договорните отношения с нея и най-малко 2 години след тяхното прекратяване.

5. Известно ми е, че за разпространението на фактите, сведенията и предметите, които са конфиденциални за Организацията, а също и за измислени и недостоверни факти, които дискредитират работещите и Организацията, или клиенти и партньори, нося наказателна отговорност от Наказателния кодекс.

6. Предупреден/а съм, че за подадени неверни данни в настоящата декларация нося отговорност по чл. 313 от НК.

Настоящата Декларация е изготвена в мое присъствие и е подписана от мен доброволно, без принуда и с ясно съзнание за всички последствия и отговорности, които нося.

ДАТА:	ДЕКЛАРАТОР:		
	ПОДПИС:	ИМЕ:	ФАМИЛИЯ: