ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ

Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org

УНИФИЦИРАН ПРОФИЛ НА ДИГИТАЛНИТЕ УМЕНИЯ ЗА КЛЮЧОВА ДЛЪЖНОСТ: **31546004 ОТГОВОРНИК, БЕЗОПАСНОСТ НА ПОЛЕТИТЕ**, СЪГЛАСНО ЕВРОПЕЙСКАТА РАМКА ЗА ДИГИТАЛНИ УМЕНИЯ DIGCOMP 2.1

Унифицираният профил е разработен по проект: BG05M9OP001-1.128-0001 "Партньорство в дигитална среда", финансиран от Оперативна програма Развитие на човешките ресурси, съфинансиран от Европейския съюз чрез Европейския социален фонд и в съответствие с Приложение 2.1 Образец на документ за описание на унифициран профил на дигиталните умения/компетентности по ключови длъжности/професии от ИЗИСКВАНИЯ към изготвянето на унифицирани профили на дигиталните умения по ключови длъжности и/или професии по НКПД 2011 и по нива и области на компетентност, съгласно Европейската рамка за дигитални умения DigComp 2.1

Код	Наименование	Кратко описание	
А. Длъжност/Професия			
A1	**Икономически сектор**	52	Складиране на товари и спомагателни дейности в транспорта
A2	**Длъжност**	31546004	Отговорник, безопасност на полетите
A3	**Алтернативни наименования на длъжността**	Началник Безопасност	
A4	**Описание на длъжността**	1. Развитие на Системата за управление на безопасността: • идентифициране на опасности, оценка на риска, разработване и прилагане на мерки за смекчаване на риска; • следи за системите за докладване, провежда вътрешни разследвания на докладвани събития и инциденти ; • следи за стойностите на индикаторите по безопасност и информира отговорния мениджър; • разработва планове за действия при аварийни ситуации и бедствия. 2. Управление на риска при извършване на промени на летището. 3. Организира работата на Комитета по безопасност, Летищния Борд по безопасност, LRST. 4. Проверки по безопасност. 5. Действия с цел подръжане на сертификата на Летище Варна по Регламент 139/2014г. на EASA. Планира, организира и инициира действия в съответствия и изискванията на EASA. 6. Планира и организира обучения по безопасност на персонала. 7. Организира извършването на инспекционни проверки на летателното поле Ниво 2. 8. Разработва и контролира изпълнението на процедури за осигуряване на безопасност при СМР на летището.	
В. Основни дигитални умения/компетентности			
B11	**Област на компетентност**	1 Грамотност, свързана с информация и данни	
B1	**Наименование и код на дигитално умение/компетентност, съгл. DigComp 2.1**	**DC13 Управление на данни, информация и дигитално съдържание**	
B12	**Описание**	Организира, съхранява и извлича данни, информация и съдържание в дигитална среда. Организира ги и ги обработва в структурирана среда.	

B13.1	**Ниво на владеене (от)**	6 - Напреднало	Способност за адаптиране към останалите в сложен контекст
B13.2	**Ниво на владеене (до)**	7 - Високо специализирано	Интегриране, с цел принос към професионалната практика и напътствие на останалите
B14.1	**Описанието на ниво на владеене (от)**	На напреднало ниво на владеене, в съответствие със собствените си нужди и тези на останалите и в сложен контекст, може да: • адаптира управлението на информация, данни и съдържание за най-подходящото и лесно извличане и съхранение; • ги адаптира за организиране и обработка в най-подходящата структурирана среда.	
B14.2	**Описанието на ниво на владеене (до)**	На високо специализирано ниво на владеене може да: • създава решения на сложни, ограничено дефинирани проблеми, които са свързани с управление на данни, информация и съдържание за тяхната организация, съхранение и извличане в структурирана дигитална среда; • интегрира знанията си, с цел да допринесе за професионалната практика и знания и да напътства останалите при управлението на данни, информация и съдържание в структурирана дигитална среда.	
B15.1	**Знания**	Познава възможностите на Системата за управление на безопасността за следене на потенциални възникнали рискове, свързани с безопасността. Познава функционалностите на системата за следене на стойностите на индикаторите по безопасност, познава методите за идентифициране на опасности и оценка на риска. Познава начини за организиране, съхраняване и извличане на данни, информация и съдържание от Системата за управление на безопасността Познава готови решения при възникване на проблеми при работа със Системата за управление на безопасността	
B15.2	**Умения**	Използва функционалностите на Системата за управление на безопасността за следене на потенциални възникнали рискове. Създава решения за справяне със сложни проблеми с множество взаимосвързани фактори, които се отнасят до управлението на данни, информация и съдържание за тяхната организация, съхранение и извличане в структурирана дигитална среда. Предлага нови идеи и процеси в съответната област. Анализира текущите възможности на системата. Предлага идеи за надграждането на Системата за управление на безопасността за следене на потенциални възникнали рискове. Отстранява неточности в базата данни. Внася актуална информация за активите и текущи събития. Обучава екипи за работа с Системата за управление на безопасността за следене на потенциални възникнали рискове. Разработва планове за действия при аварийни ситуации и бедствия.	
B15.3	**Поведения**	Самостоятелно и отговорно управлява данни, информация и дигитално съдържание в Системата за управление на безопасността за следене на потенциални възникнали рискове, при спазване на „Правилата за поверителност“ на данни.	
B16	**Примери за използване**	Пренарежда извлечената информация, по начин улесняващ нейното ефективно и пълноценно ползване от екипите	
B21	**Област на компетентност**	2 Комуникация и сътрудничество	

Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org

B2	**Наименование и код на дигитално умение/компетентност, съгл. DigComp 2.1**	**DC21 Взаимодействие чрез дигитални технологии**
B22	**Описание**	Взаимодейства чрез различни дигитални технологии и разбира подходящите дигитални средства за комуникация за даден контекст.
B23.1	**Ниво на владеене (от)**	6 - Напреднало Способност за адаптиране към останалите в сложен контекст
B23.2	**Ниво на владеене (до)**	7 - Високо специализирано Интегриране, с цел принос към професионалната практика и напътствие на останалите
B24.1	**Описанието на ниво на владеене (от)**	На напреднало ниво на владеене, в съответствие със собствените си нужди и тези на останалите и в сложен контекст, може да: • адаптира разнообразни дигитални технологии за постигане на най-удачно взаимодействие; • адаптира най-подходящите средства за комуникация за даден контекст.
B24.2	**Описанието на ниво на владеене (до)**	На високо специализирано ниво на владеене може да: • създава решения на сложни, ограничено дефинирани проблеми, които са свързани с взаимодействието чрез дигитални технологии и средства за дигитална комуникация; • интегрира знанията си, с цел да допринесе за професионалната практика и знания и да напътства останалите в процеса на взаимодействието чрез дигитални технологии.
B25.1	**Знания**	Познава функционалностите на Системата за управление на безопасността, включително възможностите за навременно докладване на потенциални рискове, както и за докладване на резултати по разследвания на събития и инциденти. Познава инструментите на системата за информиране на отговорния мениджър по всички проблеми и казуси, касаещи сигурността.
B25.2	**Умения**	Управлява Системата за управление на безопасността. Докладва за потенциални рискове, както и за резултати по разследвания на събития и инциденти чрез системата за информиране по всички проблеми и казуси, касаещи сигурността. Споделя файлове и дигитално съдържание. Комуникира с останалите членове на екипа чрез дигитални технологии. Създава и управлява съдържанието с инструментите за съвместна работа (например електронни календари, системи за управление на проекти, онлайн електронни таблици). Обсъжда ежедневни дейности на екипа с помощта на дигиталните технологии. Прави онлайн проверка на изпълнени задачи от екипа. Следи онлайн за изпълнение на работните графици на екипа. Комуникира със собственици на имоти посредством онлайн инструменти. Спазва правила за цитиране и позоваване при онлайн комуникация.
B25.3	**Поведения**	Ефективно прилага Системата за управление на безопасността, провежда вътрешни разследвания на докладвани събития и инциденти и докладва за тях на отговорния мениджър, при спазване на определени критерии.
B26	**Примери за използване**	Провеждане на вътрешни разследвания на докладвани събития и инциденти и докладване за инциденти.

C. Специфични дигитални умения/компетентности

C11	**Област на компетентност**	4 Безопасност
C1	**Наименование на дигитално умение/компетентност в свободен текст**	**Развитие на Системата за управление на безопасността в синхрон със съвременното състояние в ИТ-сектора**
C12	**Описание**	Развитие на Системата за управление на безопасността, използвайки методите за киберсигурност, като умее да идентифицира рискове и уязвимости при информационните системи и технологии, умее да се справя с компютърни заплахи и притежава компетентности при изграждането на защитни механизми и информационни политики за сигурност в организацииятa.
C13	**Сходно дигитално умение от DigComp 2.1.**	DC44 Защита на околната среда
C14.1	**Ниво на владеене (от)**	5 - Напреднало Напътствие на останалите
C14.2	**Ниво на владеене (до)**	7 - Високо специализирано Интегриране, с цел принос към професионалната практика и напътствие на останалите
C15.1	**Описанието на ниво на владеене (от)**	Умее да разрешава проблеми в областта на киберсигурността, да идентифицира рискове и уязвимости при информационните системи и технологии, да се справя с компютърни заплахи и притежава компетентности при изграждането на защитни механизми и информационни политики за сигурност в организациите.
C15.2	**Описанието на ниво на владеене (до)**	Има знания за същността на критичната инфраструктура и SCADA системите; уязвимостите на HMI, Zero day експлойти, PLC уязвимости и биометрични модалности, като притежава компетенции за работа с критична инфраструктура, SCADA системи, биометрична сигурност, биометрични системи.
C16.1	**Знания**	• Знания – за видовете компютърни заплахи, като фишинг, мрежови скенери, скенери за слаби страни, разбивачи на пароли, мрежови анализатори (sniffers), подмяна на обекти, модификация на данни, крипто вируси • Знания - за неоторизиран достъп; изтичане на информация; загуба на информация; уязвимост към кибератаки; разкриване на поверителна информация; Insider атака. DDoS атаки. • Знания – за същността на критичната инфраструктура и SCADA системите; уязвимостите на HMI, Zero day експлойти, PLC уязвимости и биометрични модалности.
C16.2	**Умения**	Контролира и регламентиране на достъпа до данните; защитава от разрушаване: антивирусна защита, контрол за автентичност на данните и програмите, защитава от хардуерни и софтуерни грешки, защитава от грешки на персонала, криптографска защита на данните. Предотвратява със Spyware, Adware, Malware, Phishing и други атаки срещу електронна поща, спам, уеб-базирани атаки Работи със SCADA, стратегии за използване на "демилитаризирани зони" (DMZ) и режими на работа на биометрични системи – идентификация и верификация.
C16.3	**Поведения**	Участва в екип заизграждане на политики и стратегии за информационна сигурност в организацията. Участва активно в утвърждаването на методи за надеждно и сигурно използване на компютърните технологии за поддържане на киберхигиена в организацията.
C17	**Примери за използване**	Успешно разрешаване на проблеми в областта на киберсигурността, чрез напътстване на останалите и утвърждава правила и методи за високоефективна киберсигурност. Идентифициране на рискове и уязвимости при информационните системи и технологии, като се справя с предотвратяването компютърни атаки и изгражда на защитни механизми и информационни политики за сигурност в организацията.

Конфедерация на независимите синдикати в България
София, 1040, пл. „Македония“ № 1, етаж 12, стая 9; тел.: 02/ 40 10 540; e-mail: mnk@knsb-bg.org