



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието

Областна дирекция „Земеделие“ – София-град

ЗАПОВЕД

№ РД – 04 – 6749

гр. София, 30.05.2023 г.

На основание чл.3, ал.3 и ал.4 от Устройствения правилник на областните дирекции „Земеделие“

УТВЪРЖДАВАМ:

1. Вътрешни правила за класификация на информацията в ОД „Земеделие“ – София-град, съгласно чл.6, ал.1 на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Утвърдените Вътрешни правила да се публикуват на интернет страницата на Областна дирекция „Земеделие“ – София-град.

Настоящата заповед да се сведе до знанието на Директора на Дирекция „Административно-правна, финансово - стопанска дейност и човешки ресурси“, Главния директор на ГД „Аграрно развитие“, главния счетоводител и началниците на общинските служби по земеделие, за сведение и изпълнение.

Контрол по изпълнение на заповедта възлагам на г-н Кристиан Венков Цветков – гл.експерт в ОД „Земеделие“ - София-град.

ИНЖ. ЯНКО ЯНКОВ

Директор на

Областна дирекция „Земеделие“

София-град



ВГ/"АПФСДЧР"



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на земеделието

Областна дирекция „Земеделие“ – София-град

УТВЪРЖДАВАМ:

ИНЖ. ЯНКО ЯНКОВ
ДИРЕКТОР НА ОД „ЗЕМЕДЕЛИЕ“ – СОФИЯ-ГРАД



**ВЪТРЕШНИ ПРАВИЛА ЗА
КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА В
ОБЛАСТНА ДИРЕКЦИЯ „ЗЕМЕДЕЛИЕ – СОФИЯ-ГРАД,
СЪГЛАСНО ЧЛ.6, АЛ. 1 НА НАРЕДБАТА ЗА
МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И
ИНФОРМАЦИОННА СИГУРНОСТ**

2023 г.

РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите правила са приети въз основа на чл. 5, ал. 1, т. 6 и 7 от Наредбата за минимални изисквания за мрежова и информационна сигурност (НМИМИС) и имат за цел да укажат как се маркира, използва, обработва, обменя, съхранява и унищожава информацията в ОД "Земеделие" – София-град.

Чл. 2 Правилата целят и гарантирането на достатъчна и адекватна защита на информацията с оглед на нейната важност и чувствителност и изпълнение на нормативните изисквания към нея.

Чл. 3 Класификацията се отразява върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията, като към тях трябва да се прилагат подходящи механизми за защита, съответстващи на идентифицираните заплахи.

Чл. 4 Служителите на ОД "Земеделие" – София-град нанасят нивото на класификацията върху документираната информация по следния начин: В горния десен ъгъл на всяка от страниците на създадения документ се изписва „ Информацията е класифицирана:“ и съответното ниво и TLP класификацията, съгласно чл. 10 и чл. 7.

Пример: „ Информацията е класифицирана:

Ниво 1, TLP-GREEN „

Чл. 5 За класификацията не се използват нивата на класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация, както и техният гриф.

Чл. 6 Информацията без класификация е достъпна за общо ползване при спазване на стандартните правила за авторски права и към нея не се прилагат механизми за защита.

Чл. 7 При обмен на информация се използва класификация TLP (traffic light protocol) съгласно Приложение № 2 към чл. 6, ал. 1 и 7 от НМИМИС.

7.1 [TLP-RED] – Само за определени получатели: в контекста на една среща например информацията се ограничава до присъстващите на срещата. В повечето случаи тази информация се предава устно или лично.

7.2 [TLP-AMBER] – Ограничено разпространение: получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът "необходимост да се знае". Честа практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.

7.3 [TLP-GREEN]– Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.

7.4 [TLP-WHITE] – Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

РАЗДЕЛ II

КЛАСИФИЦИРАНЕ НА ИНФОРМАЦИЯТА В ОД „ЗЕМЕДЕЛИЕ“ – СОФИЯ-ГРАД

Чл. 8 С цел да се гарантира достатъчна, адекватна и пропорционална на заплахите защита на информацията, се прави преценка на важността и чувствителността ѝ, както и на нормативните изисквания към нея.

Чл. 9 Въз основа на преценката по чл.9, информацията се разделя в няколко категории. Когато е приложимо, тази класификация се прилага върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето, разпространението и унищожаването на информацията, и към тях се прилагат подходящи мерки за защита, съответстващи на заплахите.

Чл. 10 В ОД “Земеделие” – София-град се определят следните на нива за класификация на информацията и изисквания към информационните и комуникационните системи за осигуряване на достъп до информацията, съгласно Приложение № 2 към чл. 6, ал. 1 и 7 от НМИМИС:

10.1 "Ниво 0" обхваща открита и общодостъпна информация (например публикувана на интернет страниците); предполага анонимно ползване на информацията и липса на средства за защита на конфиденциалността ѝ; отговаря на **TLP-WHITE**;

10.1.1 Оповестяването на информация с класификация **"Ниво 0"** не е ограничено;

10.1.2 Източниците могат да използват класификация **"Ниво 0"**, когато информацията носи минимален или никакъв предвидим риск от злоупотреба, в съответствие с приложимите правила и процедури за публично оповестяване;

10.1.3 При спазване на стандартните правила за авторски права информация с класификация **"Ниво 0"** може да се разпространява без ограничения.

10.2 "Ниво 1"

10.2.1 Споделянето на информация с класификация **"Ниво 1"** е ограничено само до дадена общност; отговаря на **TLP-GREEN**;

10.2.2 Източниците могат да използват класификация **"Ниво 1"**, когато информацията е полезна за информираността на всички участващи организации, както и за партньори от широката общност или сектор;

10.2.3 Получателите могат да споделят информация с класификация **"Ниво 1"** с партньорски организации в рамките на своя сектор или общност, но не и чрез обществено достъпни канали; информацията в тази категория може да се разпространява широко в дадена общност, но не и извън нея;

10.2.4 Изисквания към **информационните и комуникационните системи**:

10.2.4.1 Достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;

10.2.4.2 Ползвателите да се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп; за установяване на идентичността трябва да се използва защитен механизъм от типа идентификатор/парола; няма изисквания за доказателство за идентичността при регистрация;

10.2.4.3 Идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;

10.2.4.4 Доверителната изчислителна система, т. е. функционалността на информационната система, която управлява достъпа до ресурсите, трябва да поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи хода на работата;

10.2.4.5 Информационната система трябва да разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;

10.2.4.6 Защитните механизми трябва да са преминали тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.

10.3 "Ниво 2"

10.3.1 Разпространението на информация с класификация "Ниво 2" е разрешено само в рамките на организациите на участниците, обработващи, съхраняващи или обменящи информацията; отговаря на TLP-AMBER с допълнително уточнение за ограничение на достъпа;

10.3.2 Източниците могат да използват класификация "Ниво 2", когато информацията изисква защита, за да бъде ефективно обменена, и носи риск за неприкосновеността на личния живот, репутацията или операциите, ако се споделя извън съответните организации;

10.3.3 Получателите могат да споделят информация с класификация "Ниво 2" с членове на собствената си организация и с потребители или клиенти, които трябва да са запознати с нея, за да се защитят или да предотвратят допълнителни щети; източниците имат правото да определят допълнителни планирани граници на споделянето, които трябва да се спазват;

10.3.4 Изисквания към информационните и комуникационните системи - в допълнение към изискванията към предишното ниво:

10.3.4.1 Като механизъм за проверка на идентичността да се използва удостоверение за електронен подпис, независимо дали е издадено за вътрешноведомствени нужди в рамките на вътрешна инфраструктура на публичния ключ, или е издадено от външен доставчик на удостоверителни услуги;

10.3.4.2 При издаване на удостоверението издаващият орган проверява съществените данни за личността на ползвателя, без да е необходимо личното му присъствие;

10.3.4.3 Доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;

10.3.4.4 Доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.

10.4 "Ниво 3"

10.4.1 Информация с класификация "Ниво 3" не е за оповестяване и разпространението ѝ е ограничено само до участниците, обработващи, съхраняващи или обменящи информацията; отговаря на TLP-RED;

10.4.2 Източниците могат да използват класификация "Ниво 3", когато информацията не може да бъде ефективно обменена с други страни и би могла да доведе до въздействия върху неприкосновеността на личния живот, репутацията или операциите на дадена страна, ако с нея бъде злоупотребено;

10.4.3 Получателите не могат да споделят информация, маркирана с "Ниво 3", с която и да е страна извън конкретния обмен, обработка или съхранение; достъпът до информацията с класификация "Ниво 3" е ограничен само до лицата, участващи в обработката ѝ; в повечето случаи информация с класификация "Ниво 3" трябва да се предава лично;

10.4.4 Изисквания към информационните и комуникационните системи - в допълнение към изискванията към предишното ниво:

10.4.4.1 Като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;

10.4.4.2 При издаване на удостоверението да е гарантирана физическата идентичност на лицето;

10.4.4.3 Доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;

10.4.4.4 Комуникацията между потребителя и системата да се осъществява по криптирани канали, използващи протокол Transport Layer Security (TLS) поне 1.2, като минималната дължина на криптиращия ключ трябва да е поне 256 бита;

10.4.4.5 Доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

РАЗДЕЛ III

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички служители в Областна дирекция „Земеделие“ – София-град са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на настоящите правила се осъществява от на Областна дирекция „Земеделие“ – София-град, директорите на дирекции и началниците на общинските служби по земеделие.

§ 3. При неспазване на разпоредбите на настоящите вътрешни правила, служителите на Областна дирекция „Земеделие“ – София-град носят дисциплинарна отговорност по реда на Закона за държавния служител и Кодекса на труда.

§ 4. Настоящите вътрешни правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност и влизат в сила от датата на утвърждаването им със Заповед № Г.