МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО
ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО ГОРИТЕ
РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ – Р У С Е
гр.Русе,бул."Скобелев" №7,п.к.443, тел.централа 082/821 706, факс 082/821 708, e_mail:rugruse@nug.bg

УТВЪРЖДАВАМ :
Инж. Огнян Савянов
Директор на РДГ Русе

ВЪТРЕШНИ ПРАВИЛА

ЗА КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА В РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ - РУСЕ

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Тези правила определят реда за маркиране, използване, обработване, обмен, съхраняване и унищожаване на информацията, с която разполага Регионална дирекция по горите - Русе, с цел намаляване на загубите от инциденти, чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки.

(2) Правилата се прилагат за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер и определят правата и задълженията на служителите като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства.

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

Чл. 3. Класификацията по приложение № 2 към чл. 6, ал. 1 и 7 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата), приета с ПМС № 186 от 26.07.2019 г. (обн., ДВ, бр. 59 от 26.07.2019 г.), се прилага и 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. (1) Нивото на класификацията по чл. 3 се нанася по подходящ начин върху документираната в Регионална дирекция по горите - Русе информация.

(2) За класификацията не се използват нивата на класификация за сигурност на информацията по Закона за защита на класифицираната информация, както и техният гриф.

(3) 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.

(4) При обмен на информация се използва класификация TLP (traffic light protocol)

съгласно приложение № 2 от Наредбата.

РАЗДЕЛ П
КЛАСИФИКАЦИИ НА ИНФОРМАЦИЯТА

Чл. 5. (1) 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.

(2) Въз основа на тази преценка информацията се разделя в няколко категории. Когато е приложимо, тази класификация се пренася и 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. 6. При обмен на информация се използва TLP (ti:affic light protocol):

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;

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;

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;

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

Чл. 7. (1) В Регионална дирекция по горите - Русе се спазва препоръчителната класификация на информацията и изисквания към информационните и комуникационните системи за осигуряване на достъп до информацията от Наредбата:

(2) „Ниво 0":

1. 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;

2. оповестяването на информация с класификация „Ниво 0" не е ограничено;

3. 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;

4. при спазване на стандартните правила за авторски права информация с класификация „Ниво 0" може да се разпространява без ограничения.

(3) „Ниво 1 ":

1. споделянето на информация с класификация „Ниво 1" е ограничено само до дадена общност; отговаря на TLP-GREEN;

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;

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;

4. изисквания към информационните и комуникационните системи:

4.1. достъпът до точно определени обекти да бъде разрешаван на точно

определени ползватели;

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, като няма изисквания за доказателство за идентичността при регистрация;

4.3. идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;

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;

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;

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.

(4) „Ниво 2":

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;

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;

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;

4. изисквания към информационните и комуникационните системи - в допълнение към предишното ниво по ал. 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;

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

4.3. доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;

4.4. · доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.

(5) „Ниво 3":

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;

2. източниците могат да използват класификация „Ниво 3", когато информацията не може да бъде ефективно обменяна 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;

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;

4. изисквания към информационните и комуникационните системи - в

допълнение към изискванията към предишното ниво по ал. 4:

4.1. като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;

4.2. при издаване на удостоверението да е гарантирана физическата идентичност на лицето;

4.3. доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;

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;

4.5. доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

Чл. 8. Ръководителите и служителите в Регионална дирекция по горите - Русе са длъжни да познават и спазват разпоредбите на тези правила.

Чл. 9. Контролът по спазване на правилата се осъществява от директора на Регионална дирекция по горите - Русе или от определеното със заповед длъжностно лице за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в Регионална дирекция по горите - Русе. Допустими са допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.

Чл. 10. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като в дирекцията могат да се приемат и прилагат допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ **1.** Настоящите вътрешни правила влизат в сила от датата на утвърждаването им със Заповед № 30/28.02.2023 г.

§ 2. Тези вътрешни правила се изменят, допълват и отменят със заповед на директора на РДГ - Русе.