МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО
ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО ГОРИТЕ
РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ - ШУМЕН
гр. Шумен, ул. "Любен Каравелов" № 28а, п. код 9700, тел. 054/800-703, факс 054/800-704

Утвърждавам: .....
инж. Емил Гелов
Директор на РДГ Шумен

ВЪТРЕШНИ ПРАВИЛА

ЗА КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА В РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ ШУМЕН към Заповед РД05-65 от 02.04.2021 на Директора на РДГ Шумен

РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Чл. 1. (1) Тези правила определят реда за маркиране, използване, обработване, обмен, съхраняване и унищожаване на информацията, с която се работи в Регионална дирекция по горите (РДГ) Шумен, 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 по ал. 1 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 и чувствителност и спазването на съответните нормативни изисквания.

Чл. 3. Класификацията по приложение № 2 към чл. 6, ал. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата), приета с Постановление № 186 на МС от 2019 (обн., ДВ, бр. 59 от 2019 г), се прилага и върху пренасянето и унищожаването на информацията, като към тях 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 РДГ Шумен информация.

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

(4) 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.

При обмен на информация се използва класификация TLP (Traffic Light Protocol) съгласно приложение № 2 от Наредбата.

РАЗДЕЛ II

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 преглед на нормативните изисквания към нея за спазването им.

(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 (Traffic Light Protocol):

(5) [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;

(6) [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; когато получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника;

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

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

Чл. 7. (1) В РДГ Шумен се спазва препоръчителната класификация на информацията и изисквания към информационните и комуникационните системи за осигуряване на достъп до информацията от Наредбата:

(2) „Ниво 0" обхваща:

1. 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" обхваща:

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:

а) достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;

б) 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;

в) идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;

г) 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;

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

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

(8) „Ниво 2" обхваща:

(4) 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;

(5) 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;

(6) 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;

(7) изисквания към информационните и комуникационните системи - в допълнение към предишното ниво по ал. 3, т. 4:

а) 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;

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

в) доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;

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

(9) „Ниво 3" обхваща:

5. информация с класификация „Ниво 3" не е за оповестяване и разпространението й е ограничено само до участниците, обработващи, съхраняващи или обменящи информацията; отговаря на TLP-RED;

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;

(10) 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 й; в повечето случаи информация с класификация „Ниво 3" трябва да се предава лично;

(11) изисквания към информационните и комуникационните системи - в допълнение към изискванията към предишното ниво по ал. 4, т. 4:

а) като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;

б) при издаване на удостоверението да е гарантирана физическата идентичност на лицето;

в) доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;

г) 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;

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

Чл. 8. Ръководителите и служителите в РДГ Шумен са длъжни да познават и спазват разпоредбите на тези правила.

Чл. 9. Контролът по спазване на правилата се осъществява от изпълнителния директор на РДГ Шумен или от определеното със заповед длъжностно лице за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в РДГ Шумен. 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 агенцията могат да се приемат и прилагат допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.