ИНСТИТУТ ПО ОПТИЧЕСКИ МАТЕРИАЛИ И ТЕХНОЛОГИИ "АКАД. Й. МАЛИНОВСКИ"

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

Заличено на основание Регламент (ЕС) 2016/679

УТВЪРЖДАВАМ:

проф. д-р Цветанка Бабева
Директор на ИОМТ
дата: 13.04.2022 г.

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ИНСТИТУТ ПО ОПТИЧЕСКИ МАТЕРИАЛИ И ТЕХНОЛОГИИ "АКАД. ЙОРДАН МАЛИНОВСКИ“ (ИОМТ – БАН)

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите Вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 5 от Наредбата за минималните изисквания за мрежова и информационна сигурност и имат за цел осигуряването на контрол и управление на работата на информационните системи в ИНСТИТУТА ПО ОПТИЧЕСКИ МАТЕРИАЛИ И ТЕХНОЛОГИИ "АКАД. ЙОРДАН МАЛИНОВСКИ“ (ИОМТ – БАН). В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от администрацията на ИОМТ - БАН или с общо предназначение.

Чл. 2. Потребителите на информационни системи в ИОМТ - БАН са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова и информационна сигурност (ДВ, БР. 59 от 19.07.2019 г.)

РАЗДЕЛ II. КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 4. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

ал. (1) разделяне на потребителски от администраторски функции;

ал. (2) установяване на нива и достъп до информация;

ал. (3) регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

ал. (4) осъществяването на контрол от специализирани звена, респ. служители на администрацията.

Чл. 5. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез конкретно потребителско име, осигурено от Системния администратор/оторизираното за това лице, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 8. Лицата, които обработват лични данни, използват уникални пароли с достатъчна сложност, които не се записват или съхраняват онлайн.

Чл. 9. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 10. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 11. На служителите на ИОМТ - БАН, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

ал. (1) да ги използват извън рамките на служебните си задължения;

ал. (2) да ги предоставят на външни лица без да е заявена услуга.

Чл. 12. За нарушение целостта на данните се считат следните действия:

ал. (1) унищожаване на бази данни или части от тях;

ал. (2) повреждане на бази данни или части от тях;

ал. (3) вписване на невярна информация в бази данни или части от тях.

Чл. 13. При изнасяне на носители извън физическите граници на ИОМТ - БАН, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14. На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 15. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 16. След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл. 17. Събирането, подготовката и въвеждането на данни на страницата се извършва от служители на ИОМТ - БАН, определени със заповед на директора на Института. На посочените длъжностни лица се създават потребителски имена и пароли за извършване на актуализациите.

Чл. 18. Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителите, отговорни за качването им на интернет страницата на ИОМТ - БАН.

РАЗДЕЛ III. РАБОТНО МЯСТО

Чл. 19. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 20. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 21. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения обособени за целта в сградата на ИОМТ - БАН, съобразени с мерките за противопожарна защита.

Чл. 22. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа, съобразно дадените му права.

Чл. 23. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл. 24. Забранява се на външни лица работата с персоналните компютри на ИОМТ - БАН, освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на изрично определен служител от ИОМТ - БАН.

Чл. 25. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим „log off”.

Чл. 26. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор/оторизираното за това лице, който му оказва съответна техническа помощ.

Чл. 27. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Чл. 28. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само от Системния администратор/ оторизираното за това лице.

Чл. 29. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 30. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае.”

Чл. 31. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 32. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 33. Системния администратор/оторизираното за това лице извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща в ИОМТ - БАН.

Чл. 34. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл. 35. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 36. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл. 37. Компютрите, свързани в мрежата на ИОМТ - БАН използват интернет само от доставчик, с когото Институтът има сключен договор за доставка на интернет след провеждане на процедура/ред за възлагане, съгласно разпоредбите на ЗОП.

Чл. 38. Забранява се свързването на компютри едновременно в мрежата на ИОМТ - БАН и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Института и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

Чл. 39. Забранява се съхраняването на сървърите на ИОМТ - БАН на лични файлове с текст, изображения, видео и аудио.

Чл. 40. Забранява се отварянето без контрол от страна на Системния администратор/ оторизираното за това лице:

ал. (1) получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

ал. (2) получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ V. ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 41. С цел антивирусна защита се прилагат следните мерки:

ал. (1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

ал. (2) Системния администратор / оторизираното за това лице извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата.

2.2. настройва антивирусния софтуер за периодични сканирания на файловите системи на компютрите за вируси.

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система, освен в случаите когато работата с определни продукти или услуги на други институции не изискват различни настройки.

2.4. проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.

ал. (3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира Системния администратор / оторизираното за това лице.

РАЗДЕЛ VI. НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 42. Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.

2. При липса на ел. захранване за повече от 5 мин., задължително се уведомява Системния администратор / оторизираното за това лице, който при необходимст започва процедура по поетапно спиране на сървърите.

3. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

РАЗДЕЛ VII. СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 43. Системния администратор / оторизираното за това лице осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи всеки ден.

Чл. 44. Информацията, включително тази, съдържаща лични данни, се архивира по следния начин:

ал. (1) Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви.

ал. (2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър / компютър и да се продължи работният процес без чувствителна загуба на данни.

ал. (3) Честотата на архивиране на резервните копия се определя от служителите, работещи с тях и те носят отговорност за съхранението на резервните копия.

ал. (4) Резервните копия периодично се изпитват за консистентност и интегритет чрез пробно възстановяване на данни.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Ръководителите и служителите в ИОМТ - БАН са длъжни да познават и спазват разпоредбите на тези правила.

§2. Контролът по спазване на правилата се осъществява от Пом. директора АСД на ИОМТ - БАН и Системния администратор / оторизираното за това лице.

§3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ИОМТ - БАН може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§4. Тези правила са приети от Научния Съвет на ИОМТ (Протокол № 47 от 07.04.2022 г.)

§5. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.) и влизат в сила от датата на извеждане на Заповед № РД-15-147/13.04.2022 г. на директора на Института по оптически материали и технологии /ИОМТ/ Академик Й. Малиновски към БАН.

INSTITUTE OF OPTICAL MATERIALS AND TECHNOLOGIES "ACAD. J. MALINOWSKI"
BULGARIAN ACADEMY OF SCIENCES
ИНСТИТУТ ПО ОПТИЧЕСКИ МАТЕРИАЛИ И ТЕХНОЛОГИИ "АКАД. Й. МАЛИНОВСКИ"
БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
Acad. G. Bonchev Str., Bl 109, 1113 Sofia, Bulgaria
Phone/Fax:(++359-2) 872 00 73; e-mail: iomt@iomt.bas.bg; http://www.iomt.bas.bg

ЗАПОВЕД

№ РД-15-...147...../13.04.2022 г.

На основание чл. 9 от ПРАВИЛНИКА ЗА УСТРОЙСТВОТО И ДЕЙНОСТТА НА ИОМТ – БАН и чл. 1, ал. 1, т. 5 от Наредбата за минималните изисквания за мрежова и информационна сигурност

НАРЕЖДАМ:

1. Утвърждавам **ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ИНСТИТУТ ПО ОПТИЧЕСКИ МАТЕРИАЛИ И ТЕХНОЛОГИИ "АКАД. ЙОРДАН МАЛИНОВСКИ" (ИОМТ – БАН)**, които считано от датата на издаване на настоящата заповед да се прилагат в Института.

2. Правилата по т. 1, ведно с настоящата заповед да се публикуват на сайта на ИОМТ-БАН.

3. След утвърждаване на правилата по т. 1 те се прилагат в Института занапред и не пораждат действие за минали периоди.

Настоящата заповед да се доведе до знанието на всички служители в ИОМТ-БАН.

За отговорници по изпълнението на настоящата заповед определям пом. директор АСД и системния администратор в Института.

Контролът по изпълнение на заповедта ще упражнявам лично.

Заличено на основание Регламент (ЕС) 2016/679

проф. д-р Цветанка Бабева:
директор на Институт по оптически материали и технологии /ИОМТ/ Академик Й. Малиновски към БАН