ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Национална спортна академия „Васил Левски“

07 ЮНИ 2021

НСА „ВАСИЛ ЛЕВСКИ“

София 1700, ул. ”Акад. Стефан Младенов” 21, Ректорат НСА, ет.1, Деловодство ст.111	Тел. централа: (02) 40 14 100, 0898 77 66 87, 0898 77 64 40 Ректор: тел/факс (02) 400 75 04

CONTENTS

РАЗДЕЛ I. **2**

РАЗДЕЛ II. **3**

РАЗДЕЛ III **6**

РАЗДЕЛ IV **8**

РАЗДЕЛ V **10**

РАЗДЕЛ VI **11**

РАЗДЕЛ VII **12**

РАЗДЕЛ VIII **13**

РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в Национална спортна академия „Васил Левски“, град София, наричана за краткост НСА. 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 и/или глобални мрежи, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всеки факултет, всяко звено от администрацията или с общо предназначение.

Чл. 2. Потребителите на информационни системи в НСА „Васил Левски“, намиращи се на следните локации:

- Ректорат на НСА, гр. София 1700, ул. „Акад. Стефан Младенов” 21;
- Учебна сграда, ул. „Гургулят“ 1;
- Учебно-плувна база „Мадара“ – Плувен басейн Мадара (бул. „Прага” и бул. „П. Славейков”);
- Учебно-спортна водна база гр. Несебър;
- Високопланинска учебно-спортна база „Проф. Ив. Стайков” – Витоша;
- Планинска учебно-спортна база „Проф. Никола Хаджиев“ – Боровец;
- Планинска учебно-спортна база „Вихрен“,

са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършват така, че те да спазват специфичните добри практики в съответната област.

РАЗДЕЛ II

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

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

1. разделяне на потребителски от администраторски функции в домейна, като потребителските функции се разделят на обикновен потребител и десктоп потребител;
2. разделение на потребителски достъп за студенти според спецификите на съответната форма на обучение и специалност;
3. разрешаване на достъп на всеки потребител с необходимост от съответните права и не повече от необходимите такива за извършването на специфичната задача;
4. установяване на нива и достъп до информация;
5. регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
6. осъществяване на контрол от системните администратори, ръководен персонал и отговорници по сигурността, за да се обезпечи процесът на одобряване, разрешаване и изземване на съответните права и достъп до вътрешни и свързани с НСА системи и приложения.

Чл. 5. Всеки преподавател/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. Нивото на достъп не трябва да превишава специфичните за определената задача/длъжност зададени параметри. При необходимост от повишаване на нивото на достъп за определения акаунт се изисква оценка на рисковете и необходимостта от този достъп. Системните администратори анализират ситуацията, а одобрение се получава от отговорника по сигурността и/или ръководител на организацията с по-висок статут. Не се допуска едно и също лице да оценява и одобрява дадено запитване за повишаване на нивото на достъп.

Чл. 6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория, с конкретно потребителско име, осигурено от системния и/или мрежовия администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги. Въпросните лица са отговорни за водене на изрядна документация при изграждане, промяна или заличаване на активи и взаимосвързани активи.

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 на носители, лесни за компрометиране. При необходимост от боравене с множество на брой потребителски акаунти и/или пароли за достъп

организацията осигурява достатъчно надеждна система за съхранението на тези идентификационни активи, за да обезпечи тяхната защита.

Чл. 9. Всички пароли за достъп на системно ниво се променят периодично. Периодът за смяна на администраторски пароли е не по-дълъг от 90 (деветдесет) дни, а на потребители с не администраторски достъп до 180 (сто и осемдесет) дни. Допълнително се изисква всеки администратор да използва дву- или многофакторна автентификация на вход в системите на НСА.

При забравена парола тя се променя в работно време.

Чл. 10. Всички електронни 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. Ако е в електронен вариант, е необходимо поставянето на гриф за сигурност със съответното ниво на защитеност, което да гарантира, че документът и защитената от GDPR информация е достъпна и налична за обработка само от оператори на лични данни. При изтичане на зададения период, в който операторът трябва да опресни своите знания относно спазването на GDPR, правата на същия се отнемат до успешно преминат опреснителен курс /обучение.

Чл. 11. На преподавателите/служителите на НСА „Васил Левски“ от ключови служби, които използват електронни бази данни и техни производни (текстове, разпечатки, справки, дипломи и други, неописани в този раздел документи), се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения, преди да спазят предварително зададените процедури по информиране на съответните преки ръководители за намеренията си;
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица, без да е заявена услуга;
- забранено е снимането на всякакъв вид документи с лични устройства, независимо от целта и обстоятелствата, които го налагат;
- споделянето на видяна, прочетена или чута от трети лица служебна информация също се счита за нарушение на вътрешния правилник за конфиденциалност на информационните активи на НСА.

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

- унищожаване на бази данни или части от тях;
- повреждане на бази данни или части от тях;
- промяната на информация, без да има причини за това;
- вписване на невярна информация в бази данни или части от тях.

Чл. 13. При изнасяне на електронни носители извън физическите граници на НСА „Васил Левски“ те се:

- поставят в подходяща опаковка и в запечатан плик;

- води се списък с типа на изнесената информация;
- лицето, което поема отговорността за информацията извън локациите на НСА;
- цел за изнасяне на въпросната информация;
- предварително се иска разрешение за изнасяне на съответната информация, която може да изисква и оценка на риска, според преценка на отговорника по сигурността и неговия опит.

Чл. 14. На преподавателите и служителите е строго забранено да използват служебни мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Преподавателите и служителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение. При възникване на инцидент лицето, свързано с него, е задължено да уведоми съответния отговорник или отдел, които да предприемат съответните мерки за смекчаването на последствията от създалата се ситуация.

Чл. 15. Преподавателите и 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 служебна 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 или чрез машинно унищожаване. Предварително се проверяват, 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 интернет страницата на НСА се извършва от служител/служители по сключен договор за тази дейност. На посочените длъжности лица се създават потребителски имена и пароли за извършване на актуализациите, извеждане на нови съобщения и създаването на съдържание с публичен характер.

Чл. 18. Събирането и подготовката на данните се извършват от преподаватели и служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителите, отговорни за качването им на интернет страницата на НСА „Васил Левски“.

РАЗДЕЛ III

ОБОРУДВАНЕ НА РАБОТНО МЯСТО

Чл. 19. Работното място на преподавателите и служителите се оборудва с компютърна и периферна техника и други комуникационни средства. Според различните позиции, заемани в организацията, НСА може да променя – добавя или премахва, гореизброените активи според длъжностна характеристика, при специфични допълнителни задачи, водещи до необходимост за извършва на съответната задача. При необходимост от дистанционно упражняване на трудовите взаимоотношения, изграждането и поддържането на средата са задължение на служителя, като НСА е задължена да подпомогне служителя според спецификата на неговите служебни задължения.

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.). При необходимост от дистанционно упражняване на трудовите взаимоотношения, тези задължения се покриват от служителя и той носи отговорност по изграждането и осигуряването на здравословна и безопасна работна среда.

Чл. 21. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на чл. 13, чл. 24, чл. 25, чл. 29 от Наредба за минималните изисквания за мрежова и информационна сигурност (приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г). Изграждането и топологията на съответните системи се води от добрите практики и норми според БДС EN 50173-1:2018 Информационни технологии. Системи за структурно окабеляване. (Дата на публикуване: 18.09.2018 г.)

Чл. 22. Всеки преподавател/служител отговаря за целостта на компютърната и периферната 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. При настъпили промени от добрите практики и зададените изисквания на НСА той е длъжен да съобщи на съответното звено администратор и/или служител сигурност на информационните технологии за случващите се аномалии, свързани с употребата на техниката.

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. Служителят се грижи за създаването на достатъчно комплексна парола, различна от паролите, използвани за лични цели. При необходимост от подновяване на паролата той е длъжен да се води от добрите практики, зададени в НСА.

Чл. 24. Забранява се на външни лица работата с персоналните компютри на НСА „Васил Левски“, 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 служител от НСА „Васил Левски“.

Чл. 25. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off. При необходимост да се остави безнадзорно компютърната техника се заключва софтуерно режим – Lock Screen.

Чл. 26. При загуба на данни или информация от служебния компютър служителят незабавно уведомява системния администратор и/или отговорник по сигурността, които му оказват съответна техническа и/или софтуерна 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 извършват само от системен администратор.

Чл. 29. Забранява се на преподаватели и служители от служби с критична важност за институцията да използват преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на НСА „Васил Левски“.

Чл. 30. Преподавателите и служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само с преподавателите и служителите, с които имат преки служебни взаимоотношения.

Чл. 31. Архивирана компютърна информация се предоставя само на преподаватели и служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае“.

Чл. 32. 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. 33. 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. 34. Системният администратор извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на НСА „Васил Левски“. При вход в сайтове, предварително зададени в черен списък, съответният достъп може да бъде блокиран и да бъде забранен. НСА „Васил Левски“ си запазва правото да работи с бял списък с разрешени сайтове, което по презумпция води до блокиране на всички сайтове извън съответния бял списък.

Чл. 35. Ползването на компютърната мрежа и електронната поща става чрез получените потребителско име и парола. Администраторите създават правата и разрешават достъпа до отделни критични системи на база длъжностната характеристика и необходимостта от достъп до съответните активи на НСА „Васил Левски“. Оценка на риска и съответните нива на достъп следва да се проверяват на месечна база, за да се подсигури спазването на правилата и при отклонения да се отстраняват своевременно. Всяко подобно отклонение се записва в архива като инцидент със сигурността, извличат се системни логове, анализират се и се изпраща доклад към отговорника по сигурността и ръководството на НСА „Васил Левски“.

Чл. 36. Ползването на интернет и служебна електронна поща се ограничава съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на преподавателите и служителите.

Чл. 37. Преподавателите и 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. 38. Компютрите, свързани в мрежата на НСА „Васил Левски“, използват интернет само от доставчик, с който има сключен договор за доставка на интернет. Забранено е споделянето на мобилни мрежи за достъп до интернет.

Чл. 39. Забранява се свързването на компютри едновременно в мрежата на НСА „Васил Левски“ и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на НСА и/или е в противоречие с изискванията на вътрешните правила.

Чл. 40. Забраняват се инсталирането и използването на комуникатори (като icq, skype и др. подобни), ако не са от помощ на образователния процес, осигуряващи достъп извън рамките на компютърната мрежа на НСА „Васил Левски“ и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на НСА „Васил Левски“.

Чл. 41. Забранява се съхраняването на сървърите на НСА „Васил Левски“ на лични файлове с текст, изображения, видео и аудио.

Чл. 42. Забранява се отварянето без контрол от страна на системния администратор на:

- 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;
- получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ V

ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 43. С цел антивирусна защита се прилагат следните мерки:

- Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.
- Системният администратор извършва следните дейности:
    - активира защитата на съответните ресурси – файлова система, електронна поща, и извършва първоначално пълно сканиране на системата;
    - настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично;
    - активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;
    - проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.
- При поява на съобщение от антивирусната програма за вирус в локалната мрежа всеки служител от съответното работно място задължително информира системния администратор.

РАЗДЕЛ VI

НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 44. Следните мерки се прилагат с цел антивирусна защита:

- Всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.
- 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. 45. Длъжностно лице/отдел, определено от ръководството на НСА „Васил Левски“, осигурява автоматизираното създаване на резервни копия на всички бази данни и електронни документи всеки ден.

Чл. 46. Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

1. Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви.
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.
3. Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.
4. Съхраняват се най-малко последните три резервни копия.
5. Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

РАЗДЕЛ VIII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Ръководителите, преподавателите и служителите в НСА „Васил Левски“ са длъжни да познават и спазват разпоредбите на тези правила.
2. Контролът по спазване на правилата се осъществява от деканите, ръководителите на катедри, на служби, на центрове и на отдели.
3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като НСА „Васил Левски“ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията и спазването на законовите разпоредби.
4. Тези правила са разработени съгласно „НАРЕДБА за минималните изисквания за мрежова и информационна сигурност“ (приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г.).
5. Тези правила са приети с РЕШЕНИЕ НА РС – ПРОТОКОЛ № 7/07.06.2021 г.