УТВЪРДИЛ:
Ректор на НХА: /п/
ПРОФ. ГЕОРГИ ЯНКОВ

ПОЛИТИКА
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
В НАЦИОНАЛНА ХУДОЖЕСТВЕНА АКДЕМИЯ

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата политика се утвърждава на основание Закона за киберсигурност (ЗКС), приет на 31 октомври 2018 г., във връзка с чл. 4, ал. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност, приета с ПМС № 186 от 19.07.2019 г. (НМИМИС) и влиза в сила от датата на извеждане на Заповед № № 0234 – О / 23.09.2022 г. на Ректора НХА.

Чл. 2. Настоящата политика определя ред, отговорности, способи и средства при осъществяване контрол и управление на работата на информационните и комуникационните системи в НХА – съвкупността 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. Политиката съдържа стратегическите цели на НХА за мрежова и информационна сигурност и подхода за постигането им в съответствие с общите стратегически и оперативни цели на НХА, нормативните актове и договорите, текущите и потенциалните вътрешни и външни заплахи за постигането на тези цели и за сигурността на информацията.

Чл. 3. Настоящата политика задава рамката на система от мерки, насочени към:
- гарантиране на достъпност на информацията чрез осигуряване на надежден и навременен достъп;
- осигуряване на интегритет (цялост и наличност) на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
- осигуряване на конфиденциалност на информацията, чрез прилагане на одобрени ограничения върху достъпа и разкриването ѝ;
- постигане на отчетност на информацията, чрез въвеждане на контрол на достъпа и правата върху нея;
- по време на целия жизнен цикъл на информационните ресурси, включващ създаването, обработването, съхранението, пренасянето и унищожението им в и чрез информационните и комуникационните системи на НХА.

Мерките са пропорционални на рисковете за постигането на основните цели и могат да бъдат разделени най-общо на:

(1) Организационни мерки – разработване на програма за управление на информационната сигурност, да се осигури адекватното ѝ изпълнение, като се отделят необходимите ресурси и се осъществява последващ контрол.

(2) Технологични мерки – налагащи конкретни изисквания към необходими функционалности на информационните системи на НХА, приложени чрез подходящо конфигуриране, където е възможно, или чрез въвеждане на нови информационни системи.

Чл. 4. 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 НМИМИС.

Чл. 5. Длъжностно лице за мрежовата и информационната сигурност в НХА е гл. експерт

информационни технологии – ръководител на административно звено, определено със заповед на Ректора. Звеното е на пряко подчинение на Ректора и ръководителят му пряко информира Ректора за състоянието и проблемите в мрежовата и информационната сигурност.

РАЗДЕЛ II

КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 6. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:
(1) Разделяне на потребителски от администраторски функции.
(2) Установяване на нива и достъп до информация.
(3) Регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация. Използване на техниката изключително и само за служебни цели.
(4) Не се позволява инсталирането на какъвто и да е нов и преконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява ръководителя на административното звено за мрежова и информационна сигурност.
(5) Не се позволява използването на внесени отвън софтуер и хардуер.
(6) Използването на внесени отвън информационни носители (оптични дискове, флаш памети и др.) става при условие, че първо те се сканират за наличието на вируси. Ако антивирусният софтуер намери такива, носителите не се използват.
(7) Не се допускат външни лица до комуникационните шкафове и техниката за интернет връзка, с изключение на техници от оторизирани фирми, придружени от ръководителя на административното звено за мрежова и информационна сигурност.
(8) Не се допуска достъпа на външни лица до компютърната техника в канцеларииите в сградата на НХА.
(9) Служителите не могат да отстъпват паролите си за достъп до системите на НХА на други служители, външни лица, роднини и приятели.
(10) Паролите за достъп на всички служители до различните приложения и платформи се предоставят от гл. експерт информационни технологии – ръководител на административното звено за мрежова и информационна сигурност. Всички пароли за достъп на системно ниво се променят периодично.
(11) Осъществяване на контрол от ръководителя на административното звено за мрежова и информационна сигурност.

Чл. 7. Всеки служител има строго определени права на достъп и използва уникални потребителски профили за вход в системите и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 8. 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 ръководителя на административното звено за мрежова и информационна сигурност, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 9. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават права на достъп до информационните ресурси според заеманата длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 10. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 11. Всички носители на лични данни се съхраняват в безопасна и сигурна среда с ограничен и контролиран достъп.

Чл. 12. На служителите на НХА, които използват електронни бази данни и техни производни се забранява:

- да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
- да ги използват извън рамките на служебните си задължения;
- да ги предоставят на външни лица без да е заявена услуга.

Чл. 13. 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;
- вписване на невярна информация в бази данни или части от тях.

Чл. 14. При изнасяне на носители извън физическите граници на НХА, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 15. На служителите е строго забранено да използват служебни преносими устройства на места, където може да възникне риск за средството и информацията в него.

Чл. 16. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 17. 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, като предварително се проверяват, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

РАЗДЕЛ III
РАБОТНО МЯСТО

Чл. 18. Всеки служител има право да работи на служебен компютър, преносимо устройство, с компютърна и периферна техника или други комуникационни средства на своето работно място – работно помещение, работна маса и стол. Достъпът до съхраняваните данни се осъществява от него с въвеждането на персонално потребителско име и парола. Служителят отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място.

(1) След края на работния ден всеки служител задължително изключва компютъра, на който работи.

(2) При загуба на данни или информация от служебния компютър, служителят незабавно уведомява гл. експерт информационни технологии – ръководител на звеното за мрежова и информационна сигурност), който му оказва техническа помощ.

(3) 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.

(4) Забранява се използването на преносими магнитни, оптични и други носители с

възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на НХА.
(5) 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.
(6) Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача.
(7) 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.
(8) Достъпът до помещенията с комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл. 19. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърна НХА мрежи, на комуникационни устройства се извършва само след съгласуване с гл. експерт информационни технологии – ръководител на звеното за мрежова и информационна сигурност.

Чл. 20. Забранява се на външни лица работата с персоналните компютри в НХА, освен в следните случаи:

• 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 присъствието на ръководителя на звеното за мрежова и информационна сигурност.

• Провеждане на обучения на външни лица по програми и проекти е възможно след разрешение на Ректора НХА и съгласуване с ръководителя на звеното за мрежова и информационна сигурност.

РАЗДЕЛ IV
ИЗПОЛЗВАНЕ НА НАЛИЧНАТА КОМПЮТЪРНА МРЕЖА И ИНТЕРНЕТ

Чл. 21. Вътрешната мрежа с необходимите мрежови комутатори, VLAN, рутери, защитни стени, VPN и др. се изгражда от гл. експерт информационни технологии – ръководител на звеното за мрежова и информационна сигурност (или с привличане на външни експерти), който избира техническите устройства, извършва необходимите настройки.

Чл. 22. Вътрешната мрежа на НХА е разделена логически на три отделни мрежи със съответните настройки и ограничения според нивото на достъп и необходимостта от ползване:

• локална мрежа за администрация;
• локална мрежа за преподаватели;
• локална мрежа за студенти;

Чл. 23. Компютрите и комуникационните устройства, свързани в мрежата на НХА, използват интернет само от доставчик, с когото НХА има сключен договор за доставка на интернет.
Чл. 24. Ползването на компютърната и комуникационната техника на територията на НХА, както и на електронни платформи /АУИС, Google Workspace for Education, Microsoft 365 и др./ от служителите става чрез получените потребителско име и парола.

Чл. 25. Скоростта на интернета се ограничава съобразно капацитета на използвания доставчик, типа на използване – за служебни/учебни цели и за лично ползване, както и спрямо броя на работните места и свързаните към момента устройства, с цел гарантиране на непрекъсваемост на връзката за всички потребители.

Чл. 26. Служителите 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 електронните платформи при използване на предоставените им потребителски имена и пароли.

Чл. 27. Забранява се свързването на компютри едновременно в мрежата на НХА и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на НХА и/или е в противоречие с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 28. Използването на приложения за комуникация (Viber, Messenger, Facebook, Skype и др.), осигуряващи достъп извън рамките на компютърната мрежа на НХА и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер до компютрите, свързани в компютърната мрежа на НХА, следва да е ограничено само и единствено за служебна цел.

Чл. 29. Забранява се съхраняването на компютрите на НХА на лични файлове с текст, изображения, видео и аудио.

Чл. 30. Забранява се отварянето без съгласуване с ръководителя на звеното за мрежова и информационна сигурност 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.

Чл. 31. Не се толерира влизането в сайтове с неизвестно съдържание.

РАЗДЕЛ V
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 32. С цел антивирусна защита се прилагат следните мерки:

• Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява;

• Ръководителят на звеното за мрежова и информационна сигурност 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;
- активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
- проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер.

• При поява на съобщение от антивирусна програма за вирус в устройството, всеки служител задължително информира ръководителя на звеното за мрежова и информационна сигурност.

РАЗДЕЛ VI
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 33. Следните мерки се прилагат с цел непрекъсваемост на мрежовата свързаност и предотвратяването на загуба на данни:

• Всички мрежови устройства, осигуряващи интернет свързаността, както и тези за съхранение на данни, включително главен рутер, суичове, записващи устройства за видеонаблюдение, са свързани към устройство за непрекъсваемост на ел. снабдяването (UPS).

• При липса на ел. захранване за повече от 20 мин. ръководителят на звеното за мрежова и информационна сигурност започва процедура по поетапно спиране на устройствата за съхранение на данни. При срив в локалната мрежа всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация.

РАЗДЕЛ VII
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 34. Всеки служител, който работи с класифицирана/чувствителна информация, осигурява автоматично създаване на архивни копия всекидневно.

Чл. 35. Информацията, включително тази, съдържаща лични данни, се резервира по следните начини:

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

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

(3) Базите данни на следните програми се архивират всеки ден в края на работното време:

- АУИС;

РАЗДЕЛ VIII
АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл. 36. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в НХА. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл. 37. Основните понятия, част от процеса по управление на риска, са както следва:

1. конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
2. интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
3. наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл. 38. Цел на процеса за управление на риска е НХА да минимизира загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към

сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях в НХА.

Чл. 39. Методиката за управление на риска има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от НХА, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2. определяне на критериите;
3. определяне на приоритетите на риска.

Чл. 40. Анализът и оценката на риска са част от процеса за управлението му в НХА и се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл. 41. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

1. познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация; поддържащите ги системи (електрозахранващи, климатизиращи и др.); оперативни процеси/дейности; служители и външни организации), наричани за краткост "информационни активи";
2. идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
3. оценява вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;

и

4. оценява въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
5. оценява рискът за сигурността;
6. набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл. 42. При анализ и оценка на риска НХА използва регистър на рисковете (риск-регистър).

Чл. 43. В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на Наредбата:

1. информационни системи;
2. хардуерни устройства, с които са реализирани информационните системи;
3. софтуери, с които са реализирани информационните системи;
4. бази данни, включително лични данни по смисъла на GDPR;
5. записи за събитията (логове, журнали) на информационните системи;
6. документация на информационните системи (експлоатационна и потребителска);
7. комуникационни системи;
8. хардуерни устройства, с които са реализирани комуникационните системи;
9. фърмуерът на тези устройства;

10. софтуери на комуникационните системи;
11. поддържащи системи (електрозахранващи, климатични);
12. системи за контрол на физическия достъп и на околната среда;
13. процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
14. документация на тези процеси и дейности;
15. служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
16. външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;

Чл. 44. (1) За всеки от информационните активи в риск-регистъра на НХА се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.
(2) НХА отчита всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.

Чл. 45. В риск-регистъра на НХА за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл. 46. В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.

Чл. 47 (1) Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:
1. за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
2. за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.

(2) В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.

Чл. 48. За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:
1. вероятността от реализирането на заплахата е под 10 %;
2. вероятността от реализиране на заплахата е от 10 % до 30 %;
3. вероятността от реализиране на заплахата е от 30 % до 50 %;
4. вероятността от реализиране на заплахата е от 50 % до 70 %;
5. вероятността от реализиране на заплахата е над 70 %.

Чл. 49. За получаване на оценката на риска в НХА се използва следната формула: (Оценка на въздействие х Оценка на вероятност) = Оценка на риска

Чл. 50. С цел прилагане на пропорционални на заплахите механизми за защита в НХА се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложени в Наредбата.

Чл. 51. (1) Приема се, че за рискове с приоритет 3 по смисъла на Наредбата не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.
(2) За рисковете с приоритет 2 по смисъла на Наредбата се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай, че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.
(3) За всички рискове с приоритет 1 със заповед на Ректора НХА се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха и се определят срокове за прилагането им.

Чл. 52. (1) Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.
(2) гл. експерт информационни технологии организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

РАЗДЕЛ IX
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящата Политика касае и е приложима в работата на всички ръководители, служители и на работещите по договор в НХА. Потребителите на информационни системи в НХА са длъжни да познават и спазват разпоредбите на тази политика и са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

§2. Контролът по спазване на Политика се осъществява от гл. експерт информационни технологии в НХА, определен със заповед на Ректора НХА.

§3. Настоящата Политика се преразглежда и оценява периодично с оглед ефективността ѝ, но не по-рядко от веднъж годишно и при необходимост се актуализира, като НХА може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.