ВЪТРЕШНИ ПРАВИЛА

ЗА РАБОТА С ИНФОРМАЦИОННИТЕ СИСТЕМИ И КОНТРОЛНИ ДЕЙНОСТИ, СВЪРЗАНИ С ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ

В ПЛОВДИВСКИ УНИВЕРСИТЕТ “ПАИСИЙ ХИЛЕНДАРСКИ”

Организация:	ПУ "П. Хилендарски" гр. Пловдив		**Подпис:**		
Утвърдил:	Проф. д-р Румен Младенов - Ректор				
Проверил:					
Изготвил:	Проф. д-р Балик Джамбазов – Директор на УИЦ	**В действие от:**		**Брой стр.:**	11

Раздел I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Вътрешните правила за работа с информационните системи и ресурси в ПУ „Паисий Хилендарски“ имат за цел да осигурят ефективно използване на информацията от базите данни, сигурност на информационните ресурси, контрол и управление на цялостния процес по създаването, обработката, движението, използването и съхраняването на информацията в университета, свързана с неговата дейност. Използваните програмни (софтуерни) продукти и съответните бази данни могат да бъдат общи или специфични за отделните факултети, филиали или звена към Университета.

Чл. 2. Директорът на Университетския информационен център (УИЦ) е пряко отговорен за реализиране на концепцията за Пловдивски електронен университет (ПеУ). Служителите на УИЦ оказват съдействие при подготовка на информацията, подлежаща на въвеждане в съответните бази данни, разясняват програмните продукти, процедурите и конкретизират специфичните дейности, подлежащи на автоматизиране.

Чл. 3 (1). При необходимост, отделните факултети, филиали и звена могат да правят предложения до директора на УИЦ за създаване на допълнителни електронни ресурси и програмни продукти, които да осигуряват по-добра ефективност и сигурност при реализиране на тяхната дейност.

(2). Проектирането и изграждането на допълнителни/нови комуникационни и информационни системи, електронни услуги и бази данни се осъществява от УИЦ, като новите компоненти трябва да имат възможност за интеграция в единната информационна среда на Университета при спазване на Регламента за мрежовата и информационна сигурност на ПУ „Паисий Хилендарски“ и Наредбата за минималните изисквания за мрежова и информационна сигурност. Реализирането на тези дейности се утвърждава от Ректора на ПУ „Паисий Хилендарски“.

(3). За реализиране на подобни проекти, служителите на УИЦ могат да ползват консултации от други организации, учреждения и институции, които решават сходни проблеми, както и от производители и/или оторизирани дистрибутори при спазване на основните принципи за конфеденциалност.

Раздел II. БАЗИ ДАННИ

А./ Общи положения

Чл. 4. УИЦ на ПУ „Паисий Хилендарски“ поддържа различни електронни бази данни, свързани с приема на студенти и докторанти, обучението на студенти и докторанти, данни за научната, социалната, административната и финансово-управленска дейност в университета, както и данни за преподавателите и служителите на университета.

Чл. 5. Различните бази данни имат различна структура и съдържание, и се съхраняват на различни сървъри съгласно утвърдените стандарти, като веднъж седмично се прави запис на резервни копия (backup) и архивиране.

Чл. 6. Отделните действия по въвеждане на данните в информационната система (събиране, актуализиране и подреждане) се извършват съобразно организация, създадена във всяко от съответните звена. Въвеждането и актуализацията на данните в електронните бази данни се извършва от съответните служители по звена според длъжностните им характеристики и при спазване на определените права за достъп.

Чл. 7. Служителите от съответните звена, които въвеждат и актуализират електронните бази данни са длъжни да ги поддържат в актуално състояние и носят отговорност за тяхната достоверност.

Чл. 8. Обмен на информация от електронните бази данни с други организации (Министерство на образованието и науката /МОН/, Национален статистически институт, НАЦИД, Фонд „Научни изследвания“ и др.) се извършва само след одобрение от Ректора на

ПУ „Паисий Хилендарски“ при спазване на всички процедури и протоколи за сигурност при трансфер на информацията.

Чл. 9. Издаването на документи при използване на информация от електронните бази данни се извършва от съответните служители по звена съобразно длъжностните им характеристики.

Б./ Достъп до бази данни

Чл. 10. Правата за достъп до базите данни се определят съобразно длъжностните характеристики на служителите и вменените им със заповеди на Ректора задължения.

Чл. 11. Правата на достъп до бази данни за отделните звена са както следва:

(1) Въвеждане и корекция на данни, като идентифицирането на съответния служител става с дадените му потребителско име и парола за работа в локалната мрежа;

(2) Разглеждане на данните в зависимост от предмета на дейност на съответното звено и необходимата за дейността му информация, които се определят съобразно потока на информацията в Университета, мястото на съответнто звено в организационната структура, длъжностните характеристики на съответните служители и заповеди на Ректора на Университета.

Чл. 12. На служителите на Университета, които използват електронните бази данни и техни производни (текстове, разпечатки, книги и др.) се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения;

(2) да ги използват извън рамките на служебните си задължения;

(3) да ги предоставят на външни лица.

Чл. 13. За нарушение целостта на данните се считат следните действия:

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

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

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

Чл. 14. УИЦ предлага и реализира зашитата и опазването на електронните бази данни, прилагайки действащите нормативни стандарти и добри практики.

В./ Актуализация на интернет страницата на ПУ „Паисий Хилендарски“.

Чл. 15. Събирането, подготовката и въвеждането на данни директно в основните раздели на web-страницата на ПУ „Паисий Хилендаски“ (https://uni-plovdiv.bg/), се извършва от служители на УИЦ, съгласно длъжностните им характеристики и предоставените им от Директора на УИЦ администраторски права в съответствие с Регламента за мрежовата и информационна сигурност на ПУ „Паисий Хилендарски“.

Чл. 16. За някои специфични раздели на интернет страницата, служители на отделни звена събират и подготвят данните съгласно техния ресор, след което данните се качват от съответния служител (ако има предоставени права за достъп) или се предоставят в електронен вид (като файлове) на оторизираните служители от УИЦ, които поставят информацията директно на интернет страницата.

Чл. 17. Новините и информацията за предстоящи събития, които се публикуват на web-страницата на Университета задължително се одобряват от съответния ресорен отговорник преди публикуване.

Раздел III. ПРОГРАМНИ ПРОДУКТИ

Чл. 18. Системните програмни продукти се избират от УИЦ като се съобразяват както с основната дейност в Университета, а именно обучение на студенти и докторанти, така и със специфичните дейности на отделните университетски звена, осигуряващи обслужването на този процес.

Чл. 19. Програмните продукти могат да бъдат разработвани със собствени ресурси (от

програмистите в УИЦ) или да бъдат възлагани/закупувани от външни доставчици по реда на Закона за обществените поръчки (ЗОП) след предварително изготвено писмено задание, съгласувано с УИЦ и утвърдено от Ректора на Университета.

Чл. 20. Всички софтуерни продукти се съобразяват с действащите нормативни документи, свързани с електронното управление и специфичните изисквания на МОН в областта на висшето образование и поддържане на съответните електронни регистри.

Чл. 21. Функциите на приложните програми се определят и настройват в съответствие с предмета на дейност на съответното звено и изискванията на служителите, които ще работят с тях съгласно длъжностните им характеристики.

Чл. 22. Програмните менюта се визуализират с максимално възможно удобство за потребителя и при спазване на основните изисквания, посочени в 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. 23. Идентифициране и отстраняване на проблеми в работата, както и инсталация на програмни продукти, разработени от трети лица се извършва на място под контрола на УИЦ. За извършване на тези дейности може да бъде осигурен и канал за връзка, който се изгражда от УИЦ така, че да не се допусне неконтролиран достъп на външни лица до информационните системи на ПУ „Паисий Хилендарски“.

Раздел IV. ТЕХНИЧЕСКО ОСИГУРЯВАНЕ - КОМПЮТЪРНА И ПЕРИФЕРНА ТЕХНИКА

Чл. 24. Техническото осигуряване се избира според изискванията на програмните продукти, които ще се използват на съответното работно място и постиженията в развитието на компютърните технологии. Необходимата конфигурация, независимо от източника и начина на придобиване, се определя/съгласува с УИЦ.

Чл. 25. Подмяна на части, добавяне на компоненти, принадлежности и други за подобряване на компютърните конфигурации, както и текуща подмяна на дефектирала техника се извършват по преценка и разпореждане на Ръководителя на съответното звено и съгласувано с УИЦ.

Чл. 26. Инсталирането на компютърните конфигурации, системните и приложните програми, както и следващи промени в тях се прави само от служители на УИЦ или упълномощените за това фирми - доставчици на компютърна, периферна техника и програмни продукти, но задължително в присъствие на служител от УИЦ.

Чл. 27. Гаранционното обслужване на техниката се извършва само от упълномощените за това фирмени сервизи.

Чл. 28. Техническото обслужване (поддръжка), доколкото това не изисква намеса на упълномощен сервиз и дейности по ремонт, се извършва от УИЦ. При необходимост от извънгаранционен ремонт на ключово оборудване и в случай, че не е сключен договор за абонаментна поддръжка, УИЦ се свързва със сервиз, който може да осигури най-бързото и качествено възстановяване.

Чл. 29. Компютърна и периферна техника, която не се използва, се предава на УИЦ, като техниката се пренасочва към работни места, които имат нужда от такава или се предава с протокол на домакина за съхранение в определеното за тези цели помещение.

Чл. 30. Внасянето и изнасянето на компютърна и периферна техника от сградите на ПУ „Паисий Хилендарски“ става само в присъствието на служител от УИЦ или при наличие на съответния предавателно-приемателен протокол.

Раздел V. РАБОТНО МЯСТО

Чл. 31. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл. 32. 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. 33. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г). Сървърите се разполагат в помещения с осигурени постоянна температура и влажност на въздуха (поставяне на климатична инсталация) за осигуряване на подходяща за функционирането на техниката околна среда. Сървърите се разполагат така, че да не са изложени на директна слънчева светлина. В помещенията се осигуряват противопожарни средства и видеонаблюдение.

Чл. 34. 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 сървъри на локалната компютърна мрежа съобразно предоставените му права.

Чл. 35. Забранява се външни лица да имат достъп до компютри на ПУ „Паисий Хилендарски“ освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на гаранционна компютърна и периферна техника, програми, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства и сервизна намеса на място, но задължително в присъствие на служител от УИЦ.

Чл. 36. 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 след съгласуване с УИЦ.

Чл. 37. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл. 38. Всички комуникационни шкафове се заключват, като ключове от тях се намират в касата на УИЦ.

Чл. 39. В помещение, където се съхраняват електронни бази данни и програмни продукти на магнитни и магнито-оптични носители, оставането на служители в извънработно време става само при възложена конкретна задача, за чието изпълнение оставането е наложително и при спазване на разпоредбите за достъп в сградите на Университета.

Раздел VI. ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 40. Системните администратори от УИЦ извършват необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа с локалната компютърната мрежа и електронни ресурси на ПУ „Паисий Хилендарски“ според заеманата длъжност и съответните нива на достъп на служителите спазвайки приетия Регламент за мрежовата и информационна сигурност на ПУ „Паисий Хилендарски“.

Чл. 41. ПУ „Паисий Хилендарски“ предоставя свободен безжичен интернет в сградите на университета за студенти, докторанти и гости, като се прилагат допълнителни филтри.

Чл. 42 Право на служебна електронна поща имат всички студенти, докторанти, преподаватели и служители на ПУ „Паисий Хилендарски“ и неговите филиали, като получаването става автоматично след регистрация в електронния портал на университета

(https://e-portal.uni-plovdiv.bg/account/login/).

Чл. 43. При възникване на проблем с университетската мрежа, електронна поща или интернет, потребителите са длъжни да информират в рамките на 24 часа системните администратори в УИЦ или да изпратят запитване на е-мейл: support@uni-plovdiv.bg

Чл. 44. При възникване на проблем с web-страницата на университета https://uni·plovdiv.bg потребителите могат да изпратят запитване на е-мейл: webmaster@uni-plovdiv.bg

Чл. 45. Служителите от съответните факултети, филиали и звена са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на компютърната мрежа и информационни ресурси, достъпа до интернет или електронна поща чрез предоставените им потребителски имена и пароли.

Чл. 46. ПУ „Паисий Хилендарски“ осигурява непрекъснат достъп до интернет чрез сключване на договори поне с два независими доставчици. Компютрите, свързани в мрежата на Университета използват интернет само от доставчик, с когото има сключен договор.

Чл. 47. Забранява се свързването на компютри едновременно в мрежата на Университета и в други мрежи, когато това позволява разкриване и достъп до IP адреси и/или е в противоречие с изискванията на Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г., загл. изм. ДВ бр.5 от 17.01.2017 г.).

Чл. 48. На потребителите се забранява да съхраняват на сървърите на Университета лични файлове с текст, изображения, видео и аудио или да инсталират нелицензиран софтуер в определените им потребителски директории, до които имат достъп.

Чл. 49. На всички сървъри и ключови работни станции се инсталира лицензиран антивирусен софтуер.

Раздел VII. ПРАВА НА ДОСТЪП ДО ИНФОРМАЦИОННИ РЕСУРСИ

Чл. 50. Процедурите за защита на информационните системи и ресурси на ПУ „Паисий Хилендарски“ са описани в т. нар. Регламент за мрежовата и информационна сигурност на ПУ „Паисий Хилендарски“.

Чл. 51. При назначаване на нов служител или служител по заместване, отдел „Човешки ресурси“ уведомява системните администратори от УИЦ не по-късно от 3 работни дни преди датата на назначаване с оглед задаване на права на достъп до съответните локални мрежи и информационни ресурси.

Чл. 52. За промяна в правата на достъп на даден служител, ръководителят на съответното звено представя в УИЦ заявка по образец. Заявката може да се предостави и в електронен вид (по електронна поща). В случай, че основанията за промяна са документи като заповеди, длъжностна характеристика и др., УИЦ има право да изиска копия или да направи справка за съдържанието им.

Чл. 53. При прекратяване на служебното (трудовото) правоотношение между ПУ „Паисий Хилендарски“ и определен служител, отдел „Човешки ресурси“ уведомява за това системните администратори от УИЦ не по-късно от 3 работни дни преди датата на прекратяване. С изтичане на работния ден, предхождащ прекратяването на правоотношенията на служителя с Университета, се прекратяват неговите права на достъп до мрежовите и информационни ресурси, до служебни компютри, както и до служебната електронна поща. При необходимост се извършва преинсталация на използвания от служителя компютър. В определени случаи, по преценка на Директора на УИЦ, електронната поща на служителя може да остане функционална до 3 месеца след прекратяването на правоотношенията.

Чл. 54. Системните администратори прилагат задължителни мерки за автентикация, оторизация и одит на компютърните мрежи и системи. Те гарантират, че потребителските

профили са индивидуални, като в ежедневната работа трябва да се използват профили с най-ниското ниво на достъп, което дава възможност за изпълнение на съответните служебни задължения.

Чл. 55. Системните администратори правят редовни прегледи на достъпите, но не по-рядко от 4 пъти в годината. При тези прегледи се установява дали всички, на които е даден достъп до мрежата, до отделните системи и/или приложения, имат право на него в съответствие със служебните им задължения, дали външни лица имат достъп и какъв е той (бивши служители, представители на трети страни и др.).

Чл. 56. УИЦ гарантира, че достъпът до споделени файлове и принтери е разрешен само от мрежата, контролирана от УИЦ.

Чл. 57. УИЦ разработва и прилага планове за действия в случай на аварии, природни бедствия или други непредвидени обстоятелства, които биха причинили прекъсване на предоставяните услуги от Университета.

Раздел VIII. ЗАЩИТА НА ПРОФИЛИТЕ С АДМИНИСТРАТИВНИ ПРАВА ЗА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ И ТЕХНИТЕ КОМПОНЕНТИ

Чл. 58. Преди въвеждане в експлоатация на всяка система, задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив.

Чл. 59. Администраторските профили са персонални и се използват само за административни цели. Те се създават и активират чрез LDAP, използвайки служебните е-мейли на служителите, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и др.).

Чл. 60. Правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и технически периметър на всеки администратор.

Чл. 61. Данните за автентикацията на администраторските акаунти:

- са различни за всяка система;
- са с възможно най-голяма сложност, позволена от системата или нейния компонент;
- се съхраняват на физически и логически защитени сървъри, като достъп до тях има само оторизиран представител от УИЦ.

Чл. 62. УИЦ поддържа списък на администраторските профили за информационните системи, бази данни и техните компоненти. За голяма част от сървърите, паролите са съставени от 3 части (фрагментирани) като всяка част е поне 3 символа. Всеки администратор знае и е отговорен за собствения фрагмент от паролата. По този начин, достъпът до съответния сървър е възможен само в присъствие на съответните 3-ма администратори. Списъкът със сървърите и частичните пароли се съхраняват в запечатани пликове в касата на УИЦ и могат да се използват само при крайна необходимост или фосмажорни обстоятелства.

Чл. 63. Поне два пъти годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

Чл. 64. Паролите за автентикация на повечето администраторски профили се сменят задължително:

- периодично - най-малко веднъж в годината;
- при прекратяването на договорните отношения със служители или трети страни, на които тези данни са били известни;
- при пробив в мрежовата и информационната сигурност.

Раздел IX. АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл. 65. Системните администратори трябва да познава всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата за минималните изисквания за мрежова и информационна сигурност (Обн. ДВ. бр.59 от 26.07.2019 г.) - 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".

Чл. 66. Системните администратори постоянно 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.

Чл. 67. Директорът на УИЦ и системните администратори периодично оценяват вероятността от настъпване на тези събития, като вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях. Периодично се 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;

Чл. 68. Директорът на УИЦ и системните администратори оценяват риска за сигурността като набелязват мерки за смекчаване на рисковете с висок приоритет. При анализ и оценка на риска се използва регистър на рисковете (риск-регистър) съгласно препоръчителния такъв, регламентиран с Наредбата за минималните изисквания за мрежова и информационна сигурност (Обн. ДВ. бр.59 от 26.07.2019 г.), наричана по-долу за краткост Наредбата и приетия Регламент.

Чл. 69. При идентифициране на информационните активи в риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на Наредбата:

- информационни системи;
- хардуерни устройства, с които са реализирани информационните системи;
- софтуери, с които са реализирани информационните системи;
- бази данни, включително лични данни по смисъла на GDPR;
- записи за събитията (логове, журнали) на информационните системи;
- документация на информационните системи (експлоатационна и потребителска);
- комуникационни системи;
- поддържащи системи (електрозахранващи, климатични);
- системи за контрол на физическия достъп и на околната среда;
- процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
- документация на тези процеси и дейности;
- служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
- външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
- други.

Чл. 70. При идентифициране на заплахите за всеки от информационните активи в риск-регистъра се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

Разглеждат се всички потенциални заплахи, произтичащи вътре или извън университета, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.

Вероятни заплахи могат да бъдат:

- Влошаване на средствата за съхраняване
- Грешка при техническото обслужване
- Грешки при предаването
- Електромагнитна радиация
- Зловреден програмен код
- Злоупотреба с ресурси
- Използване на неразрешени програми и данни
- Кражба
- Маскиране на потребителска идентификация (нелегално проникване)
- Неоторизиран достъп до компютри, данни, услуги и приложения
- Неоторизиран достъп до средствата за съхраняване
- Неправилна (погрешна) маршрутизация/пренасочване на съобщения
- Отричане (доказуемост)
- Повреда на комуникационното оборудване и услугите
- Подслушване
- Пожар, наводнение
- Потребителска грешка
- Администраторска грешка
- Прекъсване/повреда на захранването (електричество и климатизация)
- Претоварване на трафика
- Природни бедствия
- Кибератака
- Софтуерни проблеми
- Техническа повреда (мрежа, системен хардуер)

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

Чл. 71. Оценка на въздействието

В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие - щетите (материални и нематериални), които дадена заплаха 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. 72. Оценка на вероятността

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:

а) за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;

б) 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.

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

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. 73. Оценка на риска

За получаване на оценката на риска се използва следната формула:

(Оценка на въздействие х Оценка на вероятност) = Оценка на риска

Чл. 74. Приоритизация на рисковете

С цел прилагане на пропорционални на заплахите механизми за защита, се прави приоритизация на рисковете на база на тяхната оценка и следните прагове:

Приоритет на риска	Оценка на риска
1	16 - 25
2	9 -15
3	1 – 8

Чл. 75. Смекчаване на рисковете

Приема се, че за рискове с приоритет 3 не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.

За рисковете с приоритет 2 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.

За всички рискове с приоритет 1 се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл. 76. Последващи действия

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.

УИЦ 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 X. КОНТРОЛ И КОНТРОЛНИ ДЕЙНОСТИ, СВЪРЗАНИ С ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ.

Чл. 77. Ръководителите на отделните звена контролират използването на компютърната и периферна техника, като при необходимост изясняват причините за неизползване на техниката и програмите или използването им не по предназначение и уведомяват УИЦ и Ректора с цел прилагане на съответните административни действия.

Чл. 78. УИЦ контролира изпълнението на гореизброените дейности, които засягат работата с електронни бази данни и не се контролират от други инстанции и при установяване на неизпълнение или неправомерно използване, предприема действия за възстановяване на изправността и уведомява Директора на УИЦ с цел прилагане на съответните административни действия.

Чл. 79. На периодична проверка от УИЦ подлежат:

- Компютрите относно: промени в хардуерната конфигурация, инсталирания софтуер, допълнително инсталиран софтуер, неразрешени промени в BIOS или операционната система на компютъра, като проверката се извършва поне веднъж годишно.
- Сървърите относно: лични файлове с текст, изображения, видео и аудио, нелицензиран софтуер, като проверката се извършва поне веднъж годишно.

Раздел XI. ДИСЦИПЛИИАРНА ОТГОВОРНОСТ

Чл. 80. Ако служителите са изискали закупуване на компютър, периферна техника и програмни продукти, но не ги използват или ги използват не по предназначение, Ректорът може да изисква от служителите от съответните звена писмени обяснения за причините.

При установяване на вината на служителите, последните се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 9 от Кодекса на Труда (КТ).

Чл. 81. Служители, които не поддържат актуални данните, с които работят, въведат умишлено неверни данни и създават условия за разпространяване на невярна електронна информация, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 3, 4, 7, 8 и 10 от КТ и се задължават да възстановят данните в актуално състояние.

Чл. 82. Служители на ПУ „Паисий Хилендарски“, които деинсталират, инсталират или разместват компютърни конфигурации, части от тях, периферна техника, активни и пасивни компоненти на локални компютърни мрежи както и комуникационни устройства се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 3 и 9 от КТ, а при повреда на техниката - и със заплащане на стойността на повредената техника.

Чл. 83. При установяване, че външни лица използват компютърна и периферна техника в Университета извън регламентираните в настоящите правила случаи, служителите на ПУ „Паисий Хилендарски“, допуснали това, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 3, 8 и 9 от КТ, а при установяване на повреди на техника, данни и програми - и със заплащане на стойността на повредените техника и програми, както и на разходите за възстановяване на данните.

Чл. 84. Служители на ПУ „Паисий Хилендарски“, които в установеното работно време не изпълняват служебните си задължения и поставените им задачи, а използват компютрите за компютърни игри или за друг вид дейност, която не е свързана с изпълнението на служебните им задължения, се наказват с дисциплинарно наказание за нарушения на трудовата дисциплина в съответствие с чл. 187, ал. 1 и 3 от КТ.

Чл. 85. При следващи нарушения на провинилия се служител се налагат следващите по степен дисциплинарни наказания съгласно чл. 188 от КТ.

Раздел XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила следва да се доведат до знанието на всички преподаватели и служители на ПУ „Паисий Хилендарски“ за спазване и изпълнение.

§ 3. Контролът по спазване на правилата се осъществява от ръководителите на отделните звена и Директорът на УИЦ.

§ 4. Тези правила влизат в сила от деня на утвърждаването им със заповед на Ректора.

§ 5. Настоящите правила са обект на изменения и допълнения, когато те служат за подобряване на ефективността на изпълнението им и/или третират проблеми, останали незасегнати в тях.