

**ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ**  
**“ГЕОРГИ БЕНКОВСКИ“**

Рег. № 4141/16.11.2021 г.

Заповед РД-03-675/25.10.2021 г.

**ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И  
ИНФОРМАЦИОННА СИГУРНОСТ В  
УЧИЛИЩНАТА КОМПЮТЪРНА МРЕЖА  
НА ВВВУ „ГЕОРГИ БЕНКОВСКИ“**

Долна Митрополия

2021

## **I. Основни положения**

Вътрешните правила за информационна сигурност са съвкупност от ръководни принципи, които определят методите и средствата за вземане на решения за начина на използване на информацията, информационните системи и мрежи на ВВВУ „Георги Бенковски“ и извън него, с цел недопускане на нерегламентирани действия.

**Целта** . Основна цел на е създаване, внедряване и поддържане на ефективна система за управление на мрежовата и информационна сигурност, която да осигури адекватни мерки за защита на конфиденциалността, интегритета и достъпността на информацията, информационните системи и мрежи на училищната компютърна мрежа на ВВВУ „Георги Бенковски“ (УКМ).

Допълнителни цели:

- Осигуряване на адекватно ниво на защита на информационните активи в обхвата на Вътрешните правила, чрез ранно откриване и предотвратяване на опитите за нерегламентиран достъп до информационни активи на ВВВУ „Георги Бенковски“;
- Недопускане уронване на авторитета на ВВВУ „Георги Бенковски“ пред обществеността;
- Осигуряване на достъп до надеждно защитени и достъпни електронни административни услуги за граждани и бизнеса;
- Осигуряване на достъп до информационните активи на служителите на ВВВУ „Георги Бенковски“, в зависимост от изпълняваните от тях функционални задължения;
- Контрол върху информационните активи на ВВВУ „Георги Бенковски“, за да не бъдат използвани като източник на заплаха;
- Създаване на условия за изграждане и поддържане на собствен капацитет от специалисти по мрежова и информационна сигурност чрез пряко ангажиране на всички структури от ВВВУ „Георги Бенковски“.
- Развитие и поддържане на сигурна и стабилна ИТ инфраструктура;

- Установяване на правила и процедури за приемливо използване на ИТ активите на УКМ;
- Защита и опазване на възможностите за реакция в случай на злоупотреба, загуба или неупълномощено разкриване на информация, както и при бедствия и аварии;
- Опазване репутацията и имиджа на ВВВУ „Георги Бенковски“ по отношение на сигурността на информацията в УКМ;
- Техническа реализация на защитата.

### **Основни принципи**

Те следва да се разглеждат като взаимно-допълващи се и са задължителни за спазване от всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“.

- Отговорност – за сигурността на информацията, информационните системи и мрежи отговарят всички потребители на ВВВУ „Георги Бенковски“. Всеки потребител отговаря персонално за своите действия и/или бездействия съгласно своите права и отговорности.
- Осведоменост – всички потребители са длъжни да осъзнаят необходимостта от осигуряване на сигурност на информацията, информационните системи и мрежи и да разберат, че единствено те могат да осигурят тази сигурност. В този смисъл сигурността е подвластна както на външен, така и на вътрешен риск. Служителите имат право да бъдат осведомени за щетите, които могат да бъдат нанесени на информацията, информационните системи и мрежи, които те използват.
- Демократичност – осигуряването на сигурността на информацията, информационните системи и мрежи не трябва да противоречи на основополагащите ценности на демократичното общество. В този смисъл сигурността не трябва да пречи на свободата на словото, свободният обмен на информация, осигуряването на конфиденциалност на обменяната информация

и връзката, запазването на личните данни, откритостта и информационната прозрачност.

- Етичност – служителите на са длъжни да зачитат законните интереси на своите колеги и на трети лица и/или организации. Техните действия или бездействия могат да се считат за злонамерени в случай, че са нанесени вреди. В този смисъл е важно те да положат усилия в намиране на необходимия баланс между изпълнението на своите служебни задължения и осигуряването на сигурността на информацията, информационните системи и мрежи, до които имат достъп.

- Проверимост – всички звена от администрацията на ВВВУ „Георги Бенковски“ трябва да са в състояние да представят доказателство за изпълнението на настоящите вътрешни правила за предприетите от тях мерки.

- Съпричастност – осигуряването на мрежова и информационна сигурност в ВВВУ „Георги Бенковски“ не е самоцел. Всяка една от тези структури/звена може да бъде жертва на инцидент. В този смисъл те са ангажирани в пълен обем по изпълнението на настоящата политика.

- Необходимост да се знае – достъпа на потребителите до информацията и информацията, информационните системи и мрежи в обхвата на настоящите вътрешни правила се дава единствено във връзка с изпълнение на служебните задължения и/или във връзка с изпълнение на конкретна задача.

- Предприемане на ответни мерки – всички служители на ВВВУ „Георги Бенковски“ са задължени да приемат и изпълняват препоръките на специалистите от служба „Комуникационни и информационни системи“, сектор „Дистанционно обучение“ и секция „Сигурност на информацията“ с цел предотвратяване и реагиране на инциденти, свързани със сигурността на информационните системи и мрежи. Този принцип се прилага поради мащабите на вредите, които може да предизвика инцидент със сигурността на информационните системи и мрежи.

- Оценка на риска – процеса на взаимодействие между потребителите и информационните системи и мрежи има уязвимости. Тези

уязвимости са от външен или вътрешен характер, технологични, физически или са подвластни на т. нар. „човешки фактор“. Тези уязвимости са обект на интерес за злонамерени действия. Оценката на риска позволява определянето на приемливо ниво и спомага при избора на необходимите технически средства и/или начини за реакции при кризисни ситуации.

- Управление на сигурността – обхваща всички служители на ВВВУ „Георги Бенковски“, участващи активно като страна във взаимодействието „потребител – информационна система“ или осигуряват това взаимодействие. Този процес е непрестанен, динамичен и включва анализ на риска, противодействие на атаките, разглеждане/обновяване на предприетите мерки за сигурност, мерки за възстановяване след пробиви, техническо обслужване, анализ и одит.

### **Приложимост**

Настоящите вътрешни правила се прилагат върху:

- Всички информационни активи, комуникационно оборудване и компютри, технически носители, елементи от информационни инфраструктури на други организации, привързани към УКМ;

- Всички работещи (назначени на трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“, които имат или във връзка с изпълнение на служебните задължения е необходимо да им бъде предоставен достъп до ресурси на УКМ.

В УКМ не се съдържа класифицирана информация от нива „Строго секретно“, „Секретно“, „Поверително“ и „За служебно ползване“ по смисъла на чл. 28 (1) от Закона за защита на класифицираната информация (ЗЗКИ) и поради тази причина настоящите вътрешни правила и свързаните с нея документи не обхваща сигурността на информацията, информационните системи и мрежи на ВВВУ „Георги Бенковски“ от посочените нива.

- Настоящите вътрешни правила не се отнася до информация извън УКМ, както и изтеглена от нея от официалните публични информационни

системи (WEB, FTP и др.). Информацията, качена на публичните информационни системи, трябва да е публикувана по надлежния ред.

### **Роля на администрацията на ВВВУ „Георги Бенковски“**

По отношение на настоящите вътрешни правила администрацията на ВВВУ „Георги Бенковски“ изпълнява две основни функции:

а) Собственик на УКМ и като такъв упражнява всички права и задължения по осигуряване на нейната сигурност чрез:

- Поддържане на нормалното ѝ функциониране. Тази функция се изпълнява основно чрез служба „Комуникационни и информационни системи“;

- Предоставяне и оторизиране на необходимите човешки и материални ресурси по управление и контрол на сигурността на информацията в системата, които са в нейно разпореждане;

- Създаване, актуализиране и прилагане на Вътрешните правила за информационна сигурност и свързаните с нея документи;

- Предприемане на необходимите действия за създаване и поддържане на необходимите нормативни документи, с които изискванията на настоящите вътрешни правила да станат задължение на служителите на ВВВУ „Георги Бенковски“ от всички звена;

- Отговорност за разпространение и запознаване на всички служители на ВВВУ „Георги Бенковски“ с Вътрешните правила и свързаните с нея документи.

б) Доставчик на информационни услуги – както за потребителите на УКМ във връзка с изпълнение на служебните им задължения, така и за предоставяне на електронни услуги в публичното пространство. Тази функция се осъществява чрез служба „Комуникационни и информационни системи“, сектор „Дистанционно обучение“ и назначените администратори на информационни услуги.

Възприетият подход за изграждане на политика за информационна сигурност цели:

- Осигуряване на възможност за поддържане на ниво на сигурност на УКМ по специфични правила;
- Гъвкавост по отношение на структурата на ВВВУ „Георги Бенковски“;
- Задаване на нормативна рамка по отношение на сигурността на информацията в УКМ.

### **Инструменти за постигане на целите**

1. Осигуряване на пълна поддръжка на мерките по сигурност на информацията в УКМ от страна на началника на училището.
2. Осигуряване на запознаване и сътрудничество на всички потребители на УКМ, влизащи в обхвата на Вътрешните правила.
3. Определяне на организационна структура (отговорни длъжностни лица) за управление на сигурността на информацията в УКМ.
4. Разпределяне на отговорностите за защита на информационните ресурси на УКМ между отделни длъжностни лица и организационни структури, свързани с използването и поддържането на УКМ.
5. Определяне на средства за контрол на изпълнението на изискванията на Вътрешните правила и свързаните с нея документи и при необходимост и извършване на корекции върху тях.

### **II. Ангажименти.**

Сигурността на информацията, информационните системи/услуги и мрежите в УКМ е от първостепенно значение за ВВВУ „Георги Бенковски“.

Всяко нарушение на конфиденциалността, целостта и достъпността до информационните системи и активи на ВВВУ „Георги Бенковски“ ще доведе до нарушение на работните процеси в училището. Осигуряването на непрекъснатостта на работните процеси е от изключително значение и за да се минимизират/елиминират отказите (случайни и преднамерени) е необходимо администрацията на ВВВУ „Георги Бенковски“ да е сигурна в:

- Целостта на информацията;

- Информационните системи/услуги и информацията са винаги достъпни;
- Не е нарушена конфиденциалността и винаги достъпа се извършва от оторизирани потребители, по оторизиран начин за оторизирани цели;
- Правата на администрацията на ВВВУ „Георги Бенковски“ и на служителите са защитени и не са в противоречие с нормативната уредба;
- Съхранена е репутацията на ВВВУ „Георги Бенковски“.

### **Ш. Управление на документите по сигурността.**

#### **1. Изготвяне, утвърждаване и собственост.**

Собственик на настоящия и всички свързани с него документи е ВВВУ „Георги Бенковски“. Тази функция се изпълнява чрез служба „Комуникационни и информационни системи“, която отговаря за съставянето, съгласуването и утвърждаването им, както и за нанасяне на промени в тях.

Посочените по-горе документи и промените в тях подлежат на съгласуване с началника на служба „Сигурност на информацията“ и утвърждаване от началника на училището.

Изготвянето на настоящите вътрешни правила и свързаните документи се извършва от служба „Комуникационни и информационни системи“, отговорните служители по чл. 3 от Наредбата за минималните изисквания за мрежова и информационна сигурност“ в съответствие със заповед на министъра на отбраната № ОХ-311/09.04.2020 г. и допълнително привлечени експерти по необходимост. Контролът по изготвянето на документите се извършва от заместник-началника на училището по административната част и логистиката.

#### **2. Преглед и извършване на промени в документите.**

Контролът върху рисковите фактори по сигурността на информацията и съответните мерки по ограничаване на въздействието е непрекъснат процес. Вътрешните правила и свързаните с нея документи са осигурени механизми за проверки, отчитащи промените в средата и технологиите.

Прегледът на Вътрешните правила се извършва на годишна база при липса на рискови събития през изтеклия период и по необходимост след

реални рискови събития и/или промяна на технологичната база на оборудването на УКМ с цел осигуряване на съответствие на действителното с необходимото ниво за сигурност.

Служба „Комуникационни и информационни системи“ е отговорна за събирането и обобщаването на постъпили предложения за промени, извършване на корекции в документите и тяхното съгласуване и утвърждаване.

Източници на информация за извършване на промени в Вътрешните правила са:

- Обратна връзка от заинтересовани страни;
- Резултати от наблюдения;
- Анализ на предприети проактивни или коригиращи действия;
- Промени в УКМ, които имат пряко влияние върху сигурността на информацията, като структура, техническа инфраструктура, ресурси, договорни отношения;
- Промяна на нормативна и/или законодателна рамка;
- Одитни доклади и препоръки от специалисти.

### **3. Приоритет на документите.**

Установен е следният приоритет на документите:

- a. Политика за информационна сигурност на УКМ;
- b. Всички останали документи, регламентиращи информационната сигурност, чиито списък е приложен към настоящия документ;
- c. Други разпоредителни документи, свързани със сигурността на информацията в УКМ.

## **IV. Организация и управление на контрола на информационната сигурност.**

### **1. Разпределение на отговорностите.**

Администрацията на ВВВУ „Георги Бенковски“ спазва принципа на разпределение на отговорностите и задълженията, като средство за

минимизиране на риска от случайни или умишлени злоупотреби с информационни активи на УКМ.

Отговорните длъжностни лица по информационна сигурност в УКМ могат да делегират изцяло или част от своите отговорности на други при спазване на следните условия:

- Прехвърлянето на отговорности не освобождава възлагащите от отговорността по правилно използване на съответните мерки;
- Едно лице/звено не може да има права и задължения за управление на определен информационен актив и същевременно да изпълнява функции на контролен орган по отношение на правилното му използване.

## **2. Контрол на сигурността на информацията в УКМ.**

Администрацията на ВВВУ „Георги Бенковски“ осигурява независим по отношение на непосредствените изпълнители контрол на спазването на изискванията на настоящите вътрешни правила и свързаните с нея документи.

Независимо от начина на извършване на проверките, резултатите от тях се представят в писмен вид на заместник-началника по административната част и логистиката.

Ако резултатите от проверката са незадоволителни, то констатирания несъответствията предлага пакет от коригиращи мерки, които се съгласуват със заместник-началника по административната част и логистиката, отговорните служители по чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност” и се утвърждават от началника на училището. Съгласуваните и утвърдени коригиращи мерки се предоставят за изпълнение на служба „Комуникационни и информационни системи“.

## **3. Структура за управление и контрол на сигурността на информацията.**

Администрацията на ВВВУ „Георги Бенковски“ поддържа административни и функционални отговорности по отношение изпълнението на изискванията за информационна сигурност в УКМ.

Разпределението на отговорностите по информационна сигурност в УКМ е както следва:

**(1) Началник на ВВВУ „Георги Бенковски“**

- Цялостна организация и ръководство на сигурността на информацията в УКМ;
- Утвърждаване на настоящите вътрешни правила и свързаните с нея документи, както и промените в тях;
- Издаване на заповеди, касаещи управлението, контрола и поддръжката на информационната сигурност в УКМ;
- Управление и контрол на действията на потребителите свързани с УКМ.

При изпълнението на тези задължения началника на ВВВУ „Георги Бенковски“ се подпомага от служби „Комуникационни и информационни системи“ и „Сигурност на информацията“.

**(2) Заместник-началник по административната част и логистиката**

Отговорностите му по отношение на информационната сигурност в УКМ обхващат ръководство и контрол на стопанисването и поддържането на инфраструктурата на УКМ.

- Съгласува заповеди по разпределянето на различните роли и отговорности при поддържането и администрирането на информационните активи на УКМ, както и на информационната сигурност в системата;
- Съгласува настоящите вътрешни правила и свързаните с нея документи, както и промените в тях;
- Осигурява подкрепа в рамките на ВВВУ „Георги Бенковски“ относно инициативи, свързани със сигурността на УКМ;
- Предлага или подписва (заповеди, разпореждания) за осигуряване на поддръжката на инфраструктурата на УКМ.

При изпълнение на тези задължения заместник-началника по административната част и логистиката се подпомага от служба „Комуникационни и информационни системи“.

### **(3) Началник на служба „Комуникационни и информационни системи“**

- Отговаря, докладва и подпомага действията на началника на училището и заместник-началника по административната част и логистиката по приложението на настоящата политика;
- Организира изготвянето, съгласуването и утвърждаването на документите по информационна сигурност в УКМ и промените в тях;
- Предлага за утвърждаване състава на екипите (отговорниците) за администриране на системите на УКМ, работещи на функционален принцип;
- Организира изготвянето на документи, свързани с поддръжката и осигуряването на работоспособността на УКМ;
- Отговаря за развитието и усъвършенстването на УКМ в интерес на служителите на ВВВУ „Георги Бенковски“;
- Съгласува постъпилите заявки за предоставяне на достъп до електронни услуги в мрежата за „НЕКЛАСИФИЦИРАНА“ информация на ВВВУ „Георги Бенковски“ и за предоставяне на достъп до информационни ресурси на УКМ.

### **(4) Секция „Сигурност на информацията“**

Секция „Сигурност на информацията“ отговаря непосредствено за защитата на КЛАСИФИЦИРАНАТА информация във ВВВУ „Георги Бенковски“. В изпълнението на тази своя отговорност тя следи за изпълнението на изискванията на националните закони и ведомствените нормативни документи, свързани с КЛАСИФИЦИРАНАТА информация.

Служба „Сигурност на информацията“ е отговорна за:

- Разследване на предполагаеми нарушения с КЛАСИФИЦИРАНА информация в УКМ;
- Осъществява наблюдение, оценка на заплахите и анализ на уязвимостите на УКМ;

- В случай на инцидент с КЛАСИФИЦИРАНА информация извършва процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите.
- Класифицира информационните активи на УКМ;
- (5) Служба „Комуникационни и информационни системи“
- Излъчва или предлага администраторите, отговорни за управлението и поддръжката на информационната и комуникационната инфраструктура, сървърите, компютърната мрежа, компютрите, системите за защита на информацията и информационните активи на ВВВУ „Георги Бенковски“;
- Събирането, систематизирането и въвеждането в УКМ на информация, свързана с дейностите по управление, наблюдение, оценка и контрол, както и разпространението на тази информация до потребителите на УКМ след съгласуване и утвърждаване (при спазване на принципа „необходимост да се знае“);
- Обучението, мотивацията и спазването на изискванията на документите за информационна сигурност на УКМ на служителите от ВВВУ „Георги Бенковски“;
- Спазването на изискванията по управление на информационна сигурност и прилагането им към елементите на УКМ;
- Системната поддръжка на информационните и комуникационните елементи на УКМ, които се предоставят на служителите на ВВВУ „Георги Бенковски“;
- Осигурява достъпността на услугите, максимално доближаваща се до принципа 24/7.

**(6) Служител/и по чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“ към Закона за киберсигурност**

Началникът на ВВВУ „Георги Бенковски“ издава заповед за разпределение на отговорностите на служители за гарантиране на мрежовата и информационна сигурност на използваните информационни системи

(съгласно чл. 3, ал. 2, т.2 от гореспоменатата наредба). Във ВВВУ „Георги Бенковски“ е назначен отговорен служител по мрежова и информационна сигурност. В настоящите вътрешни правила и свързаните с нея документи този служител ще бъде наричан „отговорник по сигурността“. Той отговаря за:

- Организира дейностите, свързани с постигане на мрежова и информационна сигурност на УКМ;
- Консултира ръководството на училището във връзка с информационната сигурност;
- Отговаря за защитата на интелектуалната собственост и материалните активи на ВВВУ „Георги Бенковски“ в областта на информационните и комуникационните технологии;
- Разследва и анализира инцидентите в областта на мрежовата и информационна сигурност във ВВВУ „Георги Бенковски“, реакциите при инциденти и предлага действия за подобряване на мрежовата и информационна сигурност;
- Разработва и предлага иновативни решения и архитектури за подобряване на информационната сигурност на ВВВУ „Георги Бенковски“;
- Участва в изготвянето на настоящите вътрешни правила за информационна сигурност на УКМ и на свързаните с нея документи, както и на промените в тях;
- Извършва контрол по изпълнението на Вътрешните правила и свързаните с нея документи;
- Изготвя доклади за съответствието на утвърдената с наложената политика, както и от проведени проверки/анализи на сигурността на информацията в УКМ.

#### **4. Съответствие, нарушения, реакция.**

Съответствието с тази политика е задължително за всички действие, извършвано от потребителите на УКМ във връзка с изпълнението на служебните им задължения.

Всяко действие, несъобразено с тази политика, което води до разкриване на информация извън тази за публичен достъп или нарушаване на други нейни параметри по сигурността, ангажира ръководството на ВВВУ „Георги Бенковски“ с предприемане на мерки, включително прекратяване на трудови или договорни правоотношения и възможност за съдебно преследване съгласно действащото законодателство.

При подозиране на нарушение на изискванията по настоящите вътрешни правила и на свързаните с тях документи, началника на училището и упълномощени от него лица си запазват правото да проверява всяка информация за нарушителя, генерирана или съхранявана в УКМ. Тази информация може да бъде използвана за целите на разследването и последващи действия.

В зависимост от степента на нарушението от страна на отговорните служители по чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“ или от контролиращите органи се изготвя доклад за инцидент по сигурността на информацията в УКМ, в който се описва нарушението и ангажираните лица. Правата за достъп на потребителя, който е нарушил правилата, могат да бъдат отнети за времето на разследване.

Допустимо е извършването на анализи от външни за ВВВУ „Георги Бенковски“ структури по покана от отговорника по сигурността след предварително съгласуване на параметрите на анализа със служба „Сигурност на информацията“.

## **V. Сигурност на човешките ресурси.**

Настоящият раздел урежда мерките, които ръководството на ВВВУ „Георги Бенковски“ взема по отношение на потребителите на УКМ с оглед на осигуряване на сигурността на информацията в УКМ.

Под потребители на УКМ в настоящите вътрешни правила се разбират всички работещи (назначени по трудови или служебни правоотношения) във

ВВВУ „Георги Бенковски“, както и всички бенефициенти, ползващи електронни услуги от УКМ.

Отговорност по изпълнение на задълженията по този раздел имат ръководителите на звената (структурите), чиито служители имат достъп до ИТ активи в УКМ.

Правата и задълженията на потребителите са описани подробно по направления в свързаните с настоящите вътрешни правила документи, представени в раздел XI на този документ.

### **1. Познаване на Вътрешните правила.**

- Всички потребители са задължени да се запознаят с настоящите вътрешни правила и свързаните с нея документи в касаещия ги обем. Потребителите потвърждават, че са запознати с настоящите вътрешни правила и свързаните с нея документи, и че разбират задълженията си съгласно тях чрез подписване на подадената „Заявка за предоставяне на достъп до електронни услуги в мрежата на „НЕКЛАСИФИЦИРНА“ информация на ВВВУ „Георги Бенковски“;

- Всички потребители са наясно какво представлява инцидент или нарушение на сигурността и какви действия трябва да се предприемат при възникване на такъв случай;

- Служителите са запознати с мерките, които техните ръководители могат да предприемат по отношение на тях при нарушаване на изискванията на Вътрешните правила за информационна сигурност на УКМ и на свързаните с нея документи.

### **2. Отговорности на ръководителите.**

- Ръководителите на звена (структури), чиито служители имат достъп до активи на УКМ са задължени да познават изискванията на Вътрешните правила за информационна сигурност на УКМ и на свързаните с нея документи и да разполагат по всяко време с актуални версии на тези документи;

- Подчинените им служители да бъдат инструктирани и мотивирани за изпълнението на изискванията на документите;

### **3. Назначаване, прекратяване или промяна на длъжността.**

- Ръководителите на звена, чиито служители имат достъп до ИТ активи на УКМ са длъжни при промяна или прекратяване на трудови или служебни правоотношения да предоставят в служба „Комуникационни и информационни системи“ писмено уведомление за промяна или прекратяване на достъп до информационни услуги в УКМ, подписано и съгласувано по надлежния ред;

- При назначаване на нов служител и необходимост от предоставяне на достъп до ресурси на УКМ съответния ръководител предоставя в служба „Комуникационни и информационни системи“ заявка по образец, съгласувана по надлежния ред;

- По необходимост достъпа до информационни услуги на УКМ се продължава и след края на службата (договора) чрез писмено уведомление на заместник-началника на училището по административната част и логистиката. В разрешението се посочват мотивите и срокът на удължаването. Копие от уведомлението с положителната резолюция на заместник-началника на училището по административната част и логистиката се предоставя на служба „Комуникационни и информационни системи“;

- В случаите, при които напускащ служител притежава знание за УКМ, което е от значение за сигурността на информацията и безпроблемното функциониране на информационните услуги на УКМ, ръководството на училището може да изиска от служителя документирането на това знание, а служителя се задължава да не разпространява това знание на трети страни.

## **VI. Управление на информационните активи.**

### **1. Собственост на информационните активи.**

а) Отговорност за сигурността на информационните активи носят техните собственици.

b) Собственик на ИТ инфраструктурата на УКМ е ВВВУ „Георги Бенковски“.

- Служба „Комуникационни и информационни системи“ носи отговорност за:
  - Поддържането на инфраструктурата на системно ниво;
  - Достъпността и интегритета на информацията;
  - Конфиденциалността на информацията в рамките на своите задължения;
  - Спазване на правилата и процедурите за сигурност на информацията;
  - Контрол и наблюдение на мрежовата активност и действията на администратори и потребители на УКМ;
  - Защита на информационните услуги на УКМ;
  - Идентификация, описание и поддържане на актуален регистър на информационните и комуникационните системи на УКМ.
- Сектор „Дистанционно обучение“ отговаря за:
  - Съдържанието, подредбата, представянето на информацията и осигуряването на достъп до информацията в интернет страницата на ВВВУ „Георги Бенковски“.
- Служба „Личен състав“ отговаря за:
  - Предоставяне ежемесечно на обобщена справка на служба „Комуникационни и информационни системи“ за назначените, преназначените и освободените служители и курсанти от ВВВУ „Георги Бенковски“.
- Деканата на факултета отговарят за:
  - Предоставяне ежемесечно на обобщена справка на служба „Комуникационни и информационни системи“ и сектор „Дистанционно обучение“ за записаните, прекъснали и възстановените студенти от ВВВУ „Георги Бенковски“.

c) За осигуряване на достоверност, актуалност и пълнота на информацията, съдържаща се в УКМ са въведени отговорни звена – собственици на отделни части от информацията. Във всяко звено собственик

се определят отговорни лица, които имат съответните права за четене, редактиране и премахване на информация от собствените им информационни активи.

d) Отговорността за сигурността на информацията която е изтеглена от оторизиран потребител на УКМ върху устройство за обработка и/или съхранение е изключително негова.

## **2. Допустимо използване.**

- Информационните активи се използват само по предназначение и са обект на непрекъснато наблюдение;

- Ръководството на ВВУ „Георги Бенковски“ и началника на училището приемат, че потребителите използват информационните системи на УКМ по правилния начин до появата на съмнение или доказателства за обратното. Те си запазват правото да извършват проверки за потвърждаване на сигурността на информационните и комуникационните активи на УКМ. Проверките се извършват съвместно от служба „Комуникационни и информационни системи“ и отговорните служители по чл. 3 (2) от „Наредба за минимални изисквания за мрежова и информационна сигурност“. В случаи на инциденти или съмнения за такива с КЛАСИФИЦИРАНА информация в проверката се включва и служба „Сигурност на информацията“. Ръководител на проверките е заместник-началника на училището по административната част и логистиката.

## **VII. Физическа сигурност.**

### **1. Обща информация.**

Този раздел касае принципите за прилагане на физически мерки за сигурност на активите на УКМ, които ефективно да ограничат рискове, свързани със:

(a) Злоумишлени или непреднамерени действия на хора – кражба, вандализъм, терористични действия;

(b) Аварийни събития – прегряване, огън, вода, прекъсване на електрозахранването и други вредни влияния;

(c) Природни бедствия.

## **2. Зони за сигурност на УКМ.**

За гарантиране на физическата сигурност на УКМ ръководството на ВВВУ „Георги Бенковски“ осигурява подходящи защитени зони (оборудвани помещения от сградите на училището) с определени параметри – контрол на достъпа, климатизация, електрозахранване, параметри на околната среда и защита от аварийни ситуации и природни бедствия. Защитените зони включват сървърни помещения и комуникационни центрове и разпределители.

Защитените зони в обхвата на УКМ са следните:

- Сървърно помещение в корпус А, стая 309;
- Комуникационни разпределители осигуряващи корпус Б и корпус Г
- Комуникационни разпределители в корпус курсанти, стаи 114, 214, 314 и 414.

Физическата сигурност на персоналните компютри на потребителите на УКМ и лицата по поддръжката се осигуряват от самите потребители.

## **3. Физически достъп и параметри на околната среда.**

Физическият достъп до защитените зони на УКМ се ограничава до лицата за поддръжка във връзка с изпълнение на служебните им задължения. С цел ограничаване на физическия достъп до защитените зони те могат да бъдат снабдени със системи за контрол на достъпа, но задължително се осигуряват със заключващи системи. Ключовете се съхраняват при лицата за поддръжка.

Елементите от информационната и комуникационната инфраструктура на УКМ работят във физически параметри, определени от производителите им. Тези параметри се осигуряват от системите за електрозахранване, климатизация, сигнално-охранителни системи и др.

На елементите от информационната и комуникационната инфраструктура на УКМ и на сигнално-охранителните системи се осигуряват условия за непрекъсваема работа.

Обект на защита са елементите на структурната кабелна система (СКС), използвани за нуждите на УКМ. Те са разделени на две основни групи:

- a) Оптична инфраструктура – осигуряваща привързване на елементите от УКМ, разположени в защитените зони;
- b) Медна инфраструктура – осигурява достъп на служителите на ВВВУ „Георги Бенковски“ до информационните системи и услуги на УКМ.

### **VIII. Непрекъснатата работа.**

Целта на раздела е да дефинира основните аспекти по осигуряване на непрекъснатата работа на системите на УКМ и да редуцира прекъсванията (случайни или преднамерени) до минимум.

Всички елементи на УКМ работят в следните основни режими на работа:

- 24/7 (двадесет и четири часа в денонощието, седем дни в седмицата) – на този режим на работа са всички информационни и комуникационни елементи от инфраструктурата на УКМ;
- 10 часов работен цикъл – на този работен цикъл са всички компютри на служители от ВВВУ „Георги Бенковски“, които са получили достъп до информационните активи на УКМ.

#### **1. План за възстановяване след бедствия и аварии.**

Ръководството на ВВВУ „Георги Бенковски“ счита, че мерките по осигуряването на непрекъснатостта на функционирането на елементите на УКМ при бедствия, аварии, инциденти с информационната сигурност и съмнения за такива са решаващи за непрекъснатостта на процесите в училището.

Основна система от УКМ, която е в основата на функционирането на по-голямата част от информационните системи/услуги е системата за осигуряване на директорийни услуги чрез active directory, която следва да осигурява:

- Пълна техническа процедура за възстановяване на сървърите на активната директория;
- Постигане на приемливо ниво на риск за непрекъснатостта на работните процеси във ВВВУ „Георги Бенковски“.

## **2. Резервни копия.**

Поддържането на резервни копия на елементите от информационната и комуникационната инфраструктура на УКМ е основа за интегритета на системата.

Обект на архивиране са:

- Пълна конфигурация на сървърите за услуги;
- Данни от информационните системи и услуги;
- Конфигурации на активното мрежово оборудване;
- Документи и информация, описващи информационната и комуникационната инфраструктура, функционирането, взаимодействието и защитата на УКМ.

## **IX. Общи права и задължения на служителите от ВВВУ „Георги Бенковски“.**

Служителите от ВВВУ „Георги Бенковски“ имат право:

- Да им бъде осигурен достъп до информационните и комуникационни ресурси от УКМ във връзка с изпълнение на служебните им задължения.
- На квалифицирана помощ от отговорните администратори и лица за поддръжка във връзка с използването на информационните системи и услуги на УКМ.
- Да изискват повишаване на качеството, обхвата и набора на предоставяните им информационни системи и услуги с цел подобряване на условията за изпълнение на служебните им задължения.
- Да използват предоставената им от ръководството на ВВВУ „Георги Бенковски“ компютърна техника, офис оборудване и информационни

ресурси за оторизирани или официални дейности, свързани с изпълнението на служебните задължения.

Служителите от ВВВУ „Георги Бенковски“ са длъжни:

- Да спазват изискванията на настоящите вътрешни правила и свързаните с нея документи.
- Да не допускат чрез свои действия и/или бездействия уронването на авторитета на отделни служители, структури и/или администрацията на Министерството на отбраната, Българската армия и ВВВУ „Георги Бенковски“, както и сигурността на същите при използването на информационните системи и услуги на УКМ.
- Да докладват на отговорните за администриране служители за нередности при експлоатацията и/или сигурността на отделни елементи или на УКМ като цяло.

На служителите от ВВВУ „Георги Бенковски“ се забранява:

- Създаването, обработването, съхранението и обмена на КЛАСИФИЦИРАНА информация по смисъла на чл. 28 (1) от ЗЗКИ, както и класифицирана информация на държава партньор на Република България и/или НАТО/ЕС.
- Да разгласяват информация за структурата, организацията, управлението, контрола и наблюдението на отделни информационни системи, компютърни мрежи и/или на УКМ като цяло.
- Да променят хардуерната и/или софтуерна конфигурация на предоставената им от ВВВУ „Георги Бенковски“ компютърна и офис техника, освен ако не са оторизирани за това.
- Неоторизирано използване и/или опити за такова на информационни системи, ресурси и мрежи от УКМ.

## **X. Юридически аспекти.**

### **1. Международни стандарти/документи.**

- Европейска конвенция за правата на човека и основните свободи;

- Документи на SANS институт (<http://www.sans.org>) – Information Security Policy Templates.

## **2. Национално законодателство.**

- Закон за защита на класифицираната информация;
- Закон за киберсигурност;
- Наредба за минималните изисквания за мрежова и информационна сигурност.

## **3. Ведомствени нормативни актове.**

- Правилник за устройството и дейността на ВВВУ „Георги Бенковски“;
- Заповед на началника на училището, относно определяне на служители, отговарящи за мрежовата и информационна сигурност във ВВВУ „Георги Бенковски“.

## **XI. Списък на свързаните с настоящите вътрешни правила за информационна сигурност на УКМ документи.**

1. Приложение 1 – Обща организация и управление на УКМ за създаване, обработване на неклассифицирана информация и достъп до ИНТЕРНЕТ
2. Приложение 2 – Информационни системи и услуги в УКМ
3. Приложение 3 – Правила за осигуряване на мрежов достъп до УКМ
4. Приложение 4 – Правила за организация на достъпа до Интернет
5. Приложение 5 – Изисквания към базовата конфигурация (операционна система и приложен софтуер) на персоналните работни места, включени в УКМ
6. Приложение 6 – Правила за организиране на достъпа до Интернет при използване Wi-Fi мрежата
7. Приложение 7 – Правила за „чисто работно място“
8. Приложение 8 – Правила за управление на паролите
9. Приложение 9 – Правила за използване на електронна поща в Интернет
10. Приложение 10 – Правила за използване на информационни, комуникационни ресурси и офис оборудване, собственост на ВВВУ „Георги Бенковски“

11. Приложение 11 – Правила за използване на мобилни устройства
12. Приложение 12 – Правила за използване на технически носители/устройства за съхранение на информация
13. Приложение 13 – Заявка за предоставяне на достъп до електронни услуги в мрежата за НЕКЛАСИФИЦИРАНА информация на ВВВУ „Георги Бенковски“
14. Приложение 14 - Правила за използване на компютърните зали във ВВВУ „Георги Бенковски“
15. Приложение 15 - Правила за използване на лични устройства
16. Приложение 16 - Молба за използване на лични устройства

ОБЩА ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА УКМ ЗА СЪЗДАВАНЕ,  
ОБРАБОТВАНЕ НА НЕКЛАСИФИЦИРАНА ИНФОРМАЦИЯ И ДОСТЪП  
ДО ИНТЕРНЕТ

**Общи положения**

Този документ определя общите аспекти по мрежовата и информационната сигурност в мрежата за обработване на „НЕКЛАСИФИЦИРАНА“ информация във ВВВУ „Георги Бенковски“.

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите от ВВВУ „Георги Бенковски“ с цел запазване на конфиденциалността, целостта и достъпността до информационните системи, услугите и информацията в мрежата и се минимизира възможността на трети лица да получат неправомерен достъп, както и да се осигури непрекъсваемостта на работните процеси в училището.

**Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“, които имат или желаят да получат достъп до ресурси на Училищната компютърна мрежа (УКМ), използвайки технически средства и мрежи на училището. На тези средства или мрежи **СЕ ЗАБРАНЯВА** създаване, обработване, съхранение и обмяна на класифицирана информация по смисъла на Закона за защита на класифицирана информация и правилника за прилагането му.

**Обхват**

Правилата на настоящия документ се отнася за мрежата за обработване на „НЕКЛАСИФИЦИРАНА“ информация. Елементи на мрежата за изградени в административните, учебните и спалните сгради на ВВВУ „Георги Бенковски“.

## **Собственик**

Цялата информационна и комуникационна инфраструктура, която осигурява среда за функциониране на УКМ е собственост на ВВБУ „Георги Бенковски“.

### **I. Обща организация.**

Изграждането на информационната инфраструктура се подчинява на следните принципи:

- Поддържане на инвентаризационна база на информационните системи, услугите, масивите за данни, сървъри (хардуерни и виртуални), комуникационните канали, активното мрежово оборудване, администраторите и потребителите на УКМ;
- Централно управление и наблюдение на основните и спомагателните информационни системи и услуги, приложен и системен софтуер, активно мрежово оборудване и комуникационни канали;
- Централизирано налагане на общи правила за управление на достъпа до информационните системи, услугите и данните в УКМ;
- Предоставените права за достъп на потребителите да не надвишават минимално изискуемите за изпълнение на служебните им задължения;
- Развитие и поддържане на инфраструктура, позволяваща изграждане на способности за отчетност на действията на различните групи потребители и администратори;
- Недопускане създаването, обработването, съхранението и обменянето на „КЛАСИФИЦИРАНА“ информация по смисъла на ЗЗКИ и правилника за прилагането му в мрежата на УКМ.

В процесите, свързани с администрирането, наблюдението и използването на информационните системи и услуги на УКМ, могат да бъдат дефинирани следните роли:

- a) **Собственик** – ВВБУ „Георги Бенковски“

- осигурява необходимите финансови ресурси за поддръжка и управление на УКМ;

- делегира права за контрол на сигурността;

- утвърждава настоящия документ.

**б) Отговорник по прекия контрол** – всеки ръководител на структура от ВВВУ „Георги Бенковски“

- отговаря за прилагането на изискванията на настоящия документ;

- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

**в) Отговорник по сигурността** – служител от ВВВУ „Георги Бенковски“ определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност

- определя се със заповед на началника на училището като отговорник по мрежова и информационна сигурност в изпълнение на Наредбата за минималните изисквания за мрежова и информационна сигурност;

- има делегирани права за контрол на сигурността в УКМ от „собственика“;

- участва в изготвянето на вътрешни правилата за информационна сигурност на ВВВУ „Георги Бенковски“;

- създава, адаптира, променя и поддържа настоящите правила в актуално състояние;

- осъществява методическо ръководство по прилагането на изискванията на настоящия документ;

- осъществява посредничество с групите потребители и администратори, към които този документ се отнася;

- отговаря за документирането на процедури и инструкции, които се отнасят към този документ, както и поддържането на тяхното актуално състояние;

- отговаря за обучението на групите потребители.

d) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- отговаря за изпълнението и спазването на изискванията, заложиени в този документ;

- съвместно с „отговорника по сигурността“ разследва инциденти в зоната на отговорност;

- приема сигнали от „потребителите“ при компрометиране и съмнения за компрометиране на системи и данни от УКМ;

- поддържа актуален списък на информационните системи и услуги, сървъри, активно мрежово оборудване и информационни масиви;

- отговаря за инсталирането на необходимия системен и приложен софтуер на компютрите на „потребителите“;

- отговаря за администрирането, поддръжката и осигуряването на работоспособността на системите на УКМ;

- отговаря за прилагането на настоящата вътрешни правила.

e) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- Спазват изискванията на настоящия документ.

*Забележка: Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.*

## **II. Физическа организация на мрежата.**

Компютърната мрежа на УКМ е изградена в топология тип „звезда“, като в периметъра са организирани няколко зони за сигурност, които според

възможността за достъп до различни информационни системи, услуги и Интернет могат да бъдат разделени както следва:

- Външна демилитаризирана зона – предназначена за разполагане на публични информационни системи и услуги;
- Потребителска зона (вътрешен периметър) – предназначена за осигуряване на достъп на потребителите до информационните системи и услуги на УКМ и Интернет;
- Зона за обработка на „НЕКЛАСИФИЦИРАНА“ информация и достъп до вътрешно-ведомствени информационни системи и услуги и БЕЗ достъп до Интернет;
- Зона за обработка на „НЕКЛАСИФИЦИРАНА“ информация БЕЗ достъп до вътрешно-ведомствени информационни системи и услуги и Интернет.

### **III. Управление на инфраструктурата.**

Управлението на сигурността на информацията се извършва на две нива:

- На мрежово ниво;
- На ниво достъп до информационни системи и услуги – на всяка предоставяна услуга са въведени допълнителни мерки за сигурност, като: контрол за време, ограничения и/или разрешения за достъп от работна станция и др. Тези мерки са въведени на информационни системи и услуги, които го позволяват.

Сигурността на информацията се изгражда в следните направления:

- Сигурност на периметъра;
- Мрежова сигурност;
- Сигурност в крайните точки;
- Сигурност на приложенията;
- Сигурност на данните.

Основни принципи на администрирането:

- Разпределение на отговорностите между различни администратори;
- Използване на различни профили (потребителски имена и пароли) за администриране на работните компютри на „потребителите“, свързване на различните информационни услуги и осигуряване на работата на активната директория;
- Използване на потребителски профили с минимално-необходими привилегии.

Управлението на информационната инфраструктура се извършва на две нива:

- На физическо ниво – достъп до мрежови ресурси;
- На ниво достъп до информационни системи и услуги.

#### **IV. Потребителски профили.**

Достъпа до информационните системи и услуги във УКМ и Интернет се осъществява единствено чрез индивидуални потребителски профили на служителите и обучаемите.

*Забележка: Допустимо е използването на различни потребителски профили, когато служителя изпълнява повече от една роля в процеса на поддръжка, управление и достъп до информационни системи и услуги, както и при организиран групов профил за множество служители за достъп до определена услуга.*

*Забележка: Допустимо е използването от обучаемите и техните преподаватели на общи локални потребителски профили в учебните кабинети и компютърни лаборатории единствено по време на планираните учебни занятия и единствено за цели, свързани с провеждането на тези занятия.*

Отговорността за извършените от потребителски профил действия и за сигурността на определен потребителски профил е на служителя (обучаемия),

на който във връзка с изпълнението на функционалните задължения е предоставен този профил.

Забранява се използването на чужд потребителски профил, както и предоставянето на достъп до потребителски профил от трети лица.

Потребителските профили се създават с минимално-необходимите привилегии за изпълнението на функционалните задължения от служителите (обучаемите).

Достъпът до потребителски профили на служители (обучаеми), с които се прекратяват служебните правоотношения (завършват своето обучение), се забранява в рамките на 10 (десет) дни от датата на получаване на ежемесечните справки от служба „Личен състав“ и декана на факултет „Авиационен“.

### **Конвенция за създаване на потребителски профили**

Потребителските профили биват за:

- Персонална употреба – персонални потребителски профили;
- Групова употреба – групови потребителски профили;
- Системни профили – профили за между системна комуникация.

#### Персонални потребителски профили

Конвенция:

**[един, два или три инициала (от собствено и/или бащино име)]+[фамилия]  
или [факултетен номер]**

*Забележка: За разделяне между отделните елементи от потребителския профил може да бъде използван знака точка. В определение случаи (напр. съвпадения на имена и/или инициали) могат да бъдат използвани и повече от три инициала. За служители със специфични и уникални (не повтарящи се) фамилии се допуска създаването на потребителски профил състоящ се само от фамилията на служителя.*

#### Групови потребителски профили

Такива потребителски профили не могат да бъдат използвани с цел достъп до информационни системи, услуги и сървъри. Създават се с цел

определяне на принадлежност към група (по функционален признак, за изпълнение на конкретна дейност, участие в работни групи и др.), която принадлежност позволява например да се създаде групов e-mail адрес. Имената на такива профили трябва пряко да се свързват с целите на групата.

Конвенция:

**[име услуга] + [допълнително име на услуга] ...**

Системни профили

Такива профили не могат да бъдат използвани с цел достъп до информационни системи, услуги и сървъри. Създават се с цел изграждане на достъп/обмен на информация между информационни системи/услуги.

Конвенция:

**srvc + [име на услуга] ...**

*Забележка: Паролите на системните профили трябва да отговарят на всички изисквания за паролите (регламентирани в Приложение 8 – „Правила за управление на паролите“). Отговорността за сигурността на системните профили и техните пароли е на назначения отговорен администратор на информационна система/услуга и/или сървър.*

- Забранява се разпространението, предоставянето на достъп до системните профили и техните пароли на трети лица;
- Забранява се използването на системните профили за всекидневен достъп до услуги от отговорните длъжностни лица.

**Всички изключения от конвенциите се съгласуват с отговорника по сигурността.**

## **V. Административни профили.**

Предназначението на административните профили е както следва:

- За администриране на комуникационната инфраструктура – това включва профили за настройка и управление на активно мрежово оборудване;
- За администриране на потребителски работни станции – персонални компютри на служители от ВВВУ „Георги Бенковски“ и работни

станции от учебните кабинети и компютърни лаборатории, включени към УKM. Допустимо е потребителските профили да бъдат както локални, така и профили от сървърите на „активната директория“;

- За администриране на сървъри – локални потребителски административни профили на сървърите за услуги (хардуерни и виртуални);
- За администриране на системи и услуги – административни панели/конзоли и др. на информационните системи и услуги;
- За администриране на бази данни;
- За поддръжка/управление на между системна комуникация – комуникация между процеси/услуги на различни системи, в това число и за осигуряване на допълнителна автентификация.

**Забранява се:**

- Предоставяне на административни привилегии на потребителски профили с цел изпълнение на повече от една и административни роли;
- Предоставяне на административни привилегии на потребители, освен ако това не е свързано с изпълнението на служебните им задължения;
- Предоставяне на административни привилегии на потребителски профили предназначени за всекидневна употреба;
- Използването на потребителски профили с административни привилегии за всекидневна употреба.

**Препоръка:**

Изискванията за паролите на потребителски профили с административни привилегии да надвишават определените в Приложение 8 – „Правила за управление на паролите“.

**VI. Управление на сигурността.**

Необходимо е управлението на сигурността да се извършва в следните направления:

- За вътрешен периметър – включва персонални компютри, принтери, преносими компютри и др., които получават достъп до

информационни системи и услуги от УКМ, използвайки компютърната мрежа на ВВВУ „Георги Бенковски“;

- За разширен вътрешен периметър – включва преносими компютри, мобилни устройства (“smart” телефони, таблети), които получават достъп до информационни системи и услуги от УКМ отдалечено през публичното пространство;

- За периметър на вътрешноведомствените услуги – включва сървъри (хардуерни и виртуални) на услуги, „активна директория“, система за обмен на електронна поща, система за наблюдение и контрол, архивни сървъри, справочно информационни системи и др.;

- За външен периметър – включва информационни системи и услуги на ВВВУ „Георги Бенковски“ в публичното пространство (Интернет), като: WEB сървъри, сървъри за имена, елементи на системата за обмен на електронна поща и др.;

- За системата за управление на мрежовата инфраструктура и управление на достъпа до мрежата (виртуални мрежи, маршрутизатори, комутатори).

#### **Изисквания:**

- Използване на възможностите на „активната директория“ за налагане на ограничения/забрани/настройки по сигурността на персонални компютри и сървъри чрез груповите политики;

- Групиране на обектите (компютри, потребители, сървъри, групи и др.) в „активната директория“ йерархично, по функционален признак, организационна принадлежност, предназначение и/или др.;

- На сървърите за услуги/персоналните компютри да бъде инсталиран единствено минимално изискван системен и приложен софтуер, необходим за предназначението на съответния сървър/персонален компютър;

- Ограничаване на достъпа на администраторите до сървърите/персоналните компютри на принципа „необходимост да се знае“ и

прилагане на минималните необходими привилегии за изпълнение на функционалните задължения;

- Ограничаване на достъпа на потребителите и/или групите потребители до информационните системи и услуги на принципа „необходимост да се знае“;
- Поддържане на системните/приложните обновления в актуално състояние;
- Изграждане на система за архивиране на сървъри (операционни системи и данни);
- Поддържане на актуално системно време на всички системи в периметъра;
- Конфигуриране на контейнер, от който да се инсталират системните/приложните обновления;
- Конфигуриране на време за ежедневно, автоматично спиране (shutdown) за системите (персонални компютри и сървъри), за които не е необходим 24/7 режим на работа;
- Конфигуриране на автоматични предупредителни съобщения при първоначално стартиране на всички компютри свързани към „активната директория“, като съобщението трябва да изразява принадлежност на компютърната система, ниво на класификация и кратки указания.

## **VII. Права и задължения.**

Администрирането на всички информационни системи, услуги, активно мрежово оборудване и др. е задължение и се извършва от съответните „отговорници по администрирането“. Тяхна основна задача е поддържането на системите в УКМ в режим на работа „24/7“ и извършването на методическо ръководство на „потребителите“ по отношение на предоставената им компютърна и офис техника и коректното използване на информационните услуги в УКМ.

Общото методическо ръководство по отношение на сигурността на информационните системи и услуги в УКМ се извършва от „отговорника по сигурността“. Той удостоверява промени в документите, услугите, настройките и мерките за сигурност.

„Отговорника по сигурността“ участва в изготвянето на настоящия и свързаните с него документи и прилагането (чрез „отговорниците по администрирането“) на изискванията на документите.

Всеки „потребител“ има право на достъп до информационни системи и услуги и данни в УКМ във връзка с изпълнението на служебните му задължения.

„Потребителите“ имат право на квалифицирана помощ по отношение на коректното използването на информационните системи и услуги в УКМ във връзка с изпълнението на служебните им задължения.

Всички „потребители“ от ВВВУ „Георги Бенковски“ са длъжни да спазват изискванията и препоръките наложени в този и свързаните с него документи.

Правата, задълженията и отговорностите на всички „роли“ са описани подробно в документите от настоящата вътрешни правила за информационна сигурност на УКМ и свързаните с нея документи, определящи изискванията по сигурността.

### **VIII. Физическа сигурност на УКМ.**

Елементите от УКМ понастоящем са разположени в следните помещения и етажни разпределители:

- Сървърно помещение в корпус А, стая 309;
- Комуникационни разпределители осигуряващи корпус Б и корпус Г
- Комуникационни разпределители в корпус курсанти, стаи 114,214,314 и 414.
- Комуникационни разпределители на отделни компютърни кабинети и лаборатории.

Всички посочени помещения и етажни разпределители са зони за сигурност, тъй като в тях са разположени всички елементи от комуникационната и информационната инфраструктура на УКМ. Ето защо отговорността по предпазването им е от изключително значение за сигурността на УКМ като цяло.

Всички длъжностни лица, отговорни за информационното/мрежово обслужване на служителите (обучаемите) от ВВВУ „Георги Бенковски“, са длъжни:

- Да заключват гореспоменатите помещения и разпределители след напускане/приключване на работа и не допускат трети лица да получат нерегламентиран достъп до тях;
- Да информират „отговорника по сигурността“ при компрометиране или съмнения за такова на комуникационни стаи, сървърни помещения и разпределителни шкафове;
- Да се грижат за разположеното в помещенията оборудване (активно мрежово оборудване, сървъри, маршрутизатори, дискови масиви, системи за климатизация, системи за осигуряване на непрекъснато електрическо захранване), като: осъществяват контакт със служители/фирми по обслужване на съответната техника;
- Да „заключват“ системните конзоли/desktop при приключване на работа.

**ЗАБРАНЯВА се:**

- Да се оставят без надзор трети лица в комуникационните стаи, сървърни помещения и разпределители;
- В комуникационните стаи и сървърни помещения да се съхранява информация (под формата на информационни/указателни табла), разкриваща информация, която може да спомогне компрометирането на отделни елементи на УКМ и/или на системата като цяло (например: пароли, кодове за достъп, схеми на свързване, топология на мрежата и др.).

## **IX. Наблюдение на отчетните файлове.**

Сигурността на информационната и комуникационната инфраструктура на УКМ зависи от имплементацията на предприетите мерки, анализа на тяхната ефективност и промяна с цел подобрене на нивото на сигурност.

Процеса по внедряване и поддържане на ефективно ниво на сигурност на УКМ може да се раздели на следните стъпки:

- a) Разработване на процедури за сигурност – подходящи и приложими към изградената комуникационна и информационна инфраструктура на УКМ и наложените изисквания към сигурността;
- b) Приложение на предприетите мерки;
- c) Наблюдение, анализ, реакция на зловредни действия/атаки;
- d) Тестване на нивото на сигурност, откриване на слабости и т.н.;
- e) Управление, промяна на процедурите с цел постигане на ефективно ниво на сигурността в зоната на отговорност.

С цел създаване на условия за анализ и оценка на състоянието на сигурността в зоната на отговорност е необходимо:

- изграждане на способности за регистриране на действията на „потребителите“ за всяка система;

Изисквания към съхранението на отчетните файлове:

- регистриране на опитите за автентификация (успешни и неуспешни);
- регистриране на идентичността на потребителите;
- регистриране на времето на достъпа, продължителността, клиентско работно място (IP адрес), името на достъпваната услуга на сървъра;
- минимален период на отчетните файлове – 180 (сто и осемдесет) дена;
- формат на съхранение – архивирани (tar, gzip, rar, zip);
- разделение/разпределение на отчетните файлове йерархично по функционален признак.

Източници за регистриране на действията на потребителите на УКМ и събитията за сигурността са:

- сървърите на услуги на УКМ;
- системите за управление на базите данни;
- системите за съхранение на данни;
- активното мрежово оборудване.

**Забележка:** Съхраняват се отчетните файлове на всички сървъри на информационни системи/услуги.

Препоръчително е да се използва активно мрежово оборудване (комутатори, маршрутизатори, концентратори, защитни стени, гранични шлюзове и др.), позволяващо регистриране на мрежовата активност на потребителите, и съхранение на тази информация на специализиран контейнер, с цел последващо анализиране.

Цялата отчетна информация от всички информационни системи, услуги, активно мрежово оборудване и др. е собственост на ВВВУ „Георги Бенковски“.

Всяко предоставяне на отчетна информация на трети лица/организации (например при разследване на инциденти) се съгласува с „отговорника по сигурността“ и „собственика“.

Право за конфигуриране на системите за регистриране на извършените действия имат „отговорниците по администрирането“.

**Забележка:** *допустими са отклонения от изискванията, определени в настоящия документ, относно параметрите на отчетната информация в зависимост от важността на услугата, натоварване, налично свободно място и др., но всяко отклонение от изискванията се съгласува с „отговорника по сигурността“.*

## **Наблюдение на информационната и комуникационната инфраструктура**

Цели на наблюдението на УКМ:

- планиране на мрежовите капацитети;
- установяване на „слаби“ места в мрежата с цел справяне с евентуални проблеми в бъдеще;
- проверка на предприетите мерките от Наредбата за минималните изисквания за мрежова и информационна сигурност.

„Отговорника по сигурността“ отговаря за:

- управление и прилагане на мерките за сигурност;
- определяне на параметрите на извършваното наблюдение;
- взема решения относно ескалирането на инциденти с локален характер на по-горно ниво;
- съгласува параметрите на предоставяната информация, събрана от наблюдението, на трети лица (компетентни органи) при разследването на инциденти в зоната на отговорност.

„Отговорника по администрирането“ отговаря за:

управление и изпълнение на процеса за наблюдение на системите в УКМ;

- управление на делегираните права за достъп до информацията, събрана от наблюдението;
- поддържане на система за единно системно време на всички информационни системи/услуги в УКМ;
- унищожаване на събраната информация от наблюдението след изтичането на необходимия период за съхранение;
- съхранение на събраната информация от наблюдението;
- изпълнението на етичните правила и неразпространението на информацията относно мрежовата активност на „потребителите“.

#### **ЗАБРАНЯВА СЕ:**

- извършване на наблюдение извън определените параметри и зоната на отговорност от отговорните длъжностни лица;
- разгласяването на каквато и да е информация, придобита по време на процеса по наблюдение.

**Забележка:** Допустимо е разгласяване на информация, придобита по време на процеса за наблюдение на трети лица (компетентни органи) при разследване на инциденти при условие, че това е съгласувано с „отговорника по сигурността“ и е информиран „собственика“ писмено.

### **Допълнителни изисквания**

- изграждане и поддържане на способности за контрол на входящия в „af-acad.bg“ електронен пощенски трафик (проверка за вируси, проверка за spam, блокиране на електронни съобщения, към които са прикачени изпълними файлове, като: VBS, EXE, COM, BAT и др.);
- забраняване на автоматичен RELAY на електронен пощенски трафик;
- изграждане на архив на изходящия от „AF-ACAD.BG“ електронен пощенски трафик с цел разследване на инциденти свързани с неправомерното използване на системата за обмен на електронна поща;
- изграждане на способности за контрол/забрана на достъпа от/до сайтове (IP адреси) с пропаганден, противоконституционен, антисоциален, антидемократичен, с порнографско и/или педофилски характер, както и сайтове проповядващи религиозна омраза, дискриминация, призоваващи към извършване на престъпления и други подобни.

### **Х. Анализ на риска.**

Сигурността на информацията в УКМ се състои в запазването на нейните елементи:

- Конфиденциалност – информацията се използва само от оторизираните за това лица;
- Цялостност – информацията е пълна, правилна и измененията не нарушават нейния интегритет;
- Достъпност – оторизираните лица имат достъп до информацията, когато това е необходимо.

- Прилагане на принципа – „НЕОБХОДИМОСТ ДА СЕ ЗНАЕ“

Най-важният елемент на компютърната мрежа на УКМ са сървърите (поддържащи функционирането на всички информационни системи, услуги и съхранение на данни) и активното мрежово оборудване (осигуряващи среда за изграждане на компютърната мрежа на УКМ).

Пораженията, които могат да се получат варират от чисто физическо унищожаване, до загуба на информация, кражба, злоупотреба с информация и манипулиране на същата. Всяко едно от тези поражения може да доведе до краткосрочна или дълговременна загуба на достъп до услуги или данни, както и до частично или пълно унищожение на информация или данни, а не на последно място стои и уронването на авторитета на ВВВУ „Георги Бенковски“, на отделни структури на училището и/или на отделни служители.

Ето защо защитата на системите на УКМ са от първостепенно значение за ръководството на ВВВУ „Георги Бенковски“, а изграждането на ефективни механизми за наблюдение, обновяване на системите, контрол на достъпа до цялата инфраструктура, разпознаване на зловредни действия и ефективното им противодействия, разпределение на отговорностите на длъжностните лица и стриктното им изпълнение са основа за поддържане на ефективно ниво за сигурност на УКМ.

## **XI. Преглед и поддържане на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствени регламентиращи документи.

## **XII. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е създадена електронна пощенска кутия и не спазва изискванията на настоящия документ, е обект на

дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция № И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 2

## ИНФОРМАЦИОННИ СИСТЕМИ И УСЛУГИ В УКМ

### **Общи положения**

В този документ са представени основните информационни системи и услуги на Училищната компютърна мрежа на ВВВУ „Георги Бенковски“ (УКМ).

### **Приложимост**

Този документ има информационно-справочен характер и има за цел да представи набора от информационни системи и услуги, които всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“ могат да използват при изпълнението на служебните си задължения или при обучението си.

**ЗАБЕЛЕЖКА:** Информационните системи и услуги представени в настоящия документ са предназначени за създаване, съхранение и обмен на

„НЕКЛАСИФИЦИРАНА“ информация по смисъла на Закона за защита на класифицираната информация и правилника за прилагането му.

## **I. Общи положения.**

Всички служители и обучаеми от ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

### **f) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за поддръжка и управление на УКМ;

- делегира права за контрол на сигурността;

- утвърждава настоящия документ.

### **g) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;

- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

### **h) Отговорник по сигурността – съгласно чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“**

- определя се със заповед на началника на училището като отговорник по мрежова и информационна сигурност в изпълнение на Наредбата за оперативна съвместимост и информационна сигурност;

- има делегирани права за контрол на сигурността на информационните системи и услуги на УКМ;

- отговаря за общото оперативно управление на сигурността;

- отговаря пряко за управлението на конфиденциалността, целостта и достъпността до информационните системи и услуги в мрежата;

- организира провеждането на тестове за откриване на уязвимости в информационните системи и услуги;

- осъществява взаимодействие с CERT България при инциденти със сигурността;

- разработва и поддържа настоящия документ;
- съвместно с „отговорника по администрирането“ разследва инциденти със сигурността на информацията в информационните системи и услуги в мрежата;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационните системи и услуги в мрежата;

- осъществява методическо ръководство по прилагане на изискванията на този документ.

i) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- Осъществява пряко управление на достъпа на „потребителите“ до информационните системи и услуги;

- Съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията в информационните системи и услуги в мрежата;

- Осъществява управлението на конфиденциалността, целостта и достъпността до информационните системи и услуги в мрежата;

- Поддържа необходимата архитектура на мрежата за осигуряване на софтуерното осигуряване (системно и приложно) в актуално състояние;

- Докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационните системи и услуги в мрежата;

- Участва в разработването и поддържането на настоящия документ.

j) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“;

- Спазват изискванията на настоящия документ;

- Докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата за достъп до Интернет.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

## **II. Групи информационни системи и услуги в УКМ.**

Според функционалното си предназначение информационните системи и услуги на УКМ, могат да бъдат разделени на следните основни групи:

- Информационни системи с публичен достъп;
- Вътрешно-ведомствени информационни системи;
- Информационни системи подпомагащи функционирането на УКМ;
- Системи за контрол и защита на УКМ и периметъра.

## **III. Информационни системи с публичен достъп.**

1.	e-learning.af-acad.bg	Учебна система за дистанционно обучение	TCP 80
2.	mail.af-acad.bg	Сървър за електронна поща в домейн af-acad.bg	TCP 25, 110
3.	www.af-acad.bg	Web сървър за официалната интернет страница на ВВВУ „Георги Бенковски“	TCP 80, 443
4.	infosys.af-acad.bg	Сървър за онагледяване на учебния процес	

## **IV. Вътрешно-ведомствени информационни системи.**

№	DNS име на системата	Предназначение	Услуга/Порт
1.	www1.af-acad.bg	Intranet	-

## V. Информационни системи, подпомагащи функционирането на УКМ.

№	DNS име на системата	Предназначение	Услуга/Порт
1.	-	-	-

## VI. Системи за контрол и защита на УКМ.

№	DNS име на системата	Предназначение	Услуга/Порт
1.			

## VII. Преглед и поддържане на документа.

Настоящия документ е обект на периодично обновяване.

## VIII. Преустановяване на достъп.

Преустановяването на достъп до услуга може да се извърши в един от следните случаи:

1. При преустановяване на трудовите/служебните правоотношения – пенсиониране, уволнение и др.;
2. Доброволно – при нежелание от страна на „потребителя“ да продължи да използва предоставения му достъп до информационни системи, услуги и/или мрежи във връзка с изпълнението на служебните му задължения;
3. Принудително – извършва се от „отговорника по администрирането“ при следните случаи:
  - Едностранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа, до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **ЗНАЧИТЕЛНИ** вреди на служители, структури, информационни системи и услуги, собственост на ВВВУ „Георги Бенковски“. При този случай „отговорника по администрирането“ има право едностранно да прекрати достъпа до услугата;
  - Двустранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа до която е

предоставен достъп на „потребителя“, при което има вероятност за причиняване на **НЕЗНАЧИТЕЛНИ** вреда на служители, структури, информационни системи и услуги собственост на ВВВУ „Георги Бенковски“ При този случай „отговорника по администрирането“ информира „потребителя“ за инцидента, размера на вредите, количеството необходимо време за възстановяване/отстраняване на проблема и др. След отстраняване на проблема, достъпа на „потребителя“ до услугата се възстановява;

4. Други – всяко непредвидено обстоятелство, при което няма пряка заплахата за сигурността, но достъпа на „потребителя“ до предоставяната услуга е възпрепятстван (подмяна на офис техника, временна и/или постоянна неработоспособност на същата, хардуерни и/или софтуерни проблеми и др.).

**Забележка:** В случаи по т.1, т.2 и т.4 „потребителите“ са длъжни незабавно да уведомят „отговорника по администрирането“ и да осигурят достъп на същия до предоставената им офис техника с цел коректното ѝ изключване от УКМ (форматиране, презареждане със системен и приложен софтуер и др.) и последващото връщане на техниката.

**Забележка:** В случаи по т.3 „Отговорника по администрирането“ съгласува своите действия с „отговорника по сигурността“. Всеки инцидент се документира подробно и се предоставя на „собственика“ – т.5 от Приложение 2 към чл. 28, ал.3 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

## **IX. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до информационна система, услуга и/или мрежа и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „**КЛАСИФИЦИРАНА**“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по

сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 3

## ПРАВИЛА ЗА ОСИГУРЯВАНЕ НА МРЕЖОВИ ДОСТЪП ДО УЧИЛИЩНАТА КОМПЮТЪРНА МРЕЖА

### **Общи положения**

Този документ определя правилата за осигуряване на „мрежови достъп“ на служителите и обучаемите от ВВВУ „Георги Бенковски“ до Училищната компютърна мрежа на ВВВУ „Георги Бенковски“ (УКМ).

Целта на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите от ВВВУ „Георги Бенковски“ при осигуряване на „мрежови достъп“ до училищната компютърна мрежа, при което да се запази конфиденциалността, целостта и достъпността до информационните системи, услуги и информацията в мрежата и се минимизира възможността трети лица да получат неправомерен достъп до информационната инфраструктура.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“, на които е предоставен достъп до информационни системи, услуги, активно комуникационно оборудване и мрежови канали, осигуряващи информационния обмен в училищната компютърна мрежа.

Правилата от настоящия документ се отнасят за мрежата за обработване на „НЕКЛАСИФИЦИРАНА“ информация.

Компютърната мрежа, осигуряваща достъп до информационните системи и услуги на училищната компютърна мрежа е собственост на ВВВУ „Георги Бенковски“.

## **I. Обща организация.**

Осигуряването на достъп до мрежата на УКМ се осъществява с цел подпомагане на отделните структурни звена от ВВВУ „Георги Бенковски“ при изпълнение на ежедневните им дейности.

### **к) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за закупуване, поддръжка и управление на мрежата на УКМ;
- делегира права за контрол на сигурността в мрежата на УКМ;
- утвърждава настоящия документ.

### **л) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

### **м) Отговорник по сигурността – съгласно чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“**

- определя се със заповед на началника на училището като отговорник по мрежова и информационна сигурност в изпълнение на Наредба за минималните изисквания за мрежова и информационна сигурност;

- има делегирани права за контрол на сигурността в мрежата на УКМ;
- отговаря за общото оперативно управление на сигурността на мрежата на УКМ;
- отговаря пряко за управлението на конфиденциалността, целостта и достъпността до информационните системи, услуги и мрежата на УКМ;
- осъществява взаимодействие с CERT България при инциденти със сигурността;
- съвместно с „отговорника по администрирането“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата на УКМ;
- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационните системи, услугите и мрежата на УКМ;
- осъществява методическо ръководство по прилагане на изискванията на този документ.

п) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- осъществява пряко управление на достъпа (включване/изключване) на „потребителите“ към Училищната компютърна мрежа;
- осъществява пряко управление на трафичните капацитети за достъп до информационните системи, услугите и мрежата на УКМ;
- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата на УКМ;
- осъществява управлението на конфиденциалността, целостта и достъпността до информационните системи, услугите и мрежата на УКМ;

- поддържа необходимата архитектура на мрежата за осигуряване на софтуерното осигуряване (системно и приложно) в актуално състояние;
- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационните системи, услугите и мрежата на УКМ;
- участва в разработването и поддържането на изискванията на настоящия документ.

о) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“:

- спазват изискванията на настоящия документ;
- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата на УКМ.

*Забележка: Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.*

## **II. Права и задължения.**

### ***Права и задължения на „собственика“:***

- делегира права на „отговорника по сигурността“ за осъществяване на пряк контрол по изпълнението на изискванията на настоящия документ;
- одобрява и осигурява необходимите финансови средства за изпълнението на мерките за сигурност, заложи в настоящия документ;

### ***Права и задължения на „отговорника по сигурността“:***

- отговаря за общото оперативно управление на сигурността на мрежата на УКМ;
- организира провеждането на тестове за откриване на уязвимости в информационните системи, услугите и мрежата на УКМ;

- осъществява пряко процеса по управление на инциденти със сигурността на информацията в Училищната компютърна мрежа;
- организира и ръководи прилагането на мерки за сигурност, както и тяхната проверка и валидиране;
- разработва и поддържа изискванията на настоящия документ;
- осъществява методическо ръководство на структурните звена от ВВУ „Георги Бенковски“ в процеса на прилагане на изискванията на настоящия документ;
- незабавно информира служителя по сигурността на информацията във ВВУ „Георги Бенковски“ при инциденти с „КЛАСИФИЦИРАНА“ информация. Подпомага служителя по сигурността на информацията при разследването на подобни инциденти.

Всички „потребители“ от ВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

а) Осигуряване на достъп до мрежата

- всеки „потребител“ има право да му бъде осигурен достъп до Училищната компютърна мрежа във връзка с изпълнение на ежедневните му дейности. Това право се определя от административния ръководител на „потребителя“ по установения ред. За обучаемите това право се заявява от ръководителя на катедрата (директора на ДПХН или ПСК), в която е необходимо да бъде предоставен достъп. Достъп се предоставя след като административния ръководител/ръководител на катедра направи заявка в служба „Комуникационни и информационни системи“ или да изпрати писмо с описание на проблема на [cis@af-acad.bg](mailto:cis@af-acad.bg).
- всеки „потребител“ има право на квалифицирана помощ от „отговорника по администрирането“ във връзка с предоставения му достъп до Училищната компютърна мрежа. За целта е необходимо да направи заявка или да изпрати писмо с описание на проблема на [cis@af-acad.bg](mailto:cis@af-acad.bg);
- осъществяването на физическото включване/изключване на мрежови устройства, услуги, системи, както и пренасочването, спирането,

агрегирането на трафик и др. е изключително право и се осъществява единствено от „отговорниците по администрирането“;

- физическото разширение/промяна на компютърната мрежа (включване/изключване на комутатори, концентратори, маршрутизатори, повторители, точки за безжичен достъп и др.) е изключително право и се осъществява единствено от „отговорниците по администрирането“.

На „потребителите“ се **ЗАБРАНЯВА**:

- включването на каквито и да е устройства (комутатори, концентратори, маршрутизатори, повторители, точки за безжичен достъп и др.), услуги, системи, както и пренасочването, спирането, агрегирането на трафик и др.;

- действия, които променят архитектурата и създават условия за компрометиране на Училищната компютърна мрежа.

*Забележка: Допустимо е използването на виртуални частни мрежи (VPN) от „отговорника по администрирането“ при осигуряването на „мрежови достъп“, с цел осигуряване и поддръжка на по-високо ниво на сигурност. Всички параметри на „мрежовия достъп“ „отговорника по администрирането“ съгласува с „отговорника по сигурността“.*

b) Контрол на мрежовата инфраструктура и трафичните капацитети

- управлението на IP адресното пространство (вътрешна мрежа и предоставени публични адреси), DNS имена на сървъри и услуги и трафичните капацитети е изключително право и се осъществява единствено от „отговорниците по администрирането“;

- всяка промяна на IP адресното пространство, DNS имена на сървъри и услуги и трафичните капацитети се съгласува с „отговорниците по сигурността“;

- „отговорниците по администрирането“ имат изключителното право да прекратят предоставен достъп до УКМ на потребители и/или системи

при установяване на нерегламентиран трафик от/до информационни системи, както и при прекомерно използване на трафичните капацитети на мрежата.

с) Заплахи за конфиденциалността, целостта и достъпността до мрежата

- в случай на заплаха към конфиденциалността, целостта или достъпността, установен нерегламентиран трафик, мрежата/система е станала източник на SPAM или др., „отговорника по администрирането“ информира „отговорника по сигурността“. „Отговорникът по администрирането“ има право да:

- придобие пълни права върху хардуер/софтуер, за да предприеме необходимите действия за установяване на проблема и неговото отстраняване;
- временно или за постоянно да преустанови достъпа до мрежата на УKM на проблемен хардуер/софтуер;
- по необходимост да спре хардуерни или софтуерни системи, цялата или части от нея до установяване и/или отстраняване на проблема.

*Забележка: Всички действия, които могат да бъдат предприети се извършват с изричното уведомяване на собственика/отговорника на хардуерното/софтуерното оборудване, съответния „отговорник по прекия контрол“.*

Възстановяването на услугите/достъпа се извършва от „отговорника по администрирането“ след пълното отстраняване/възстановяване на проблемния хардуер/софтуер.

d) Тестване на мрежата

- с цел повишаване на нивото на сигурност „отговорника по администрирането“ има право периодично и по необходимост да провежда различни тестове и сканирания на мрежата за уязвимости в мрежата на УKM;
- допустимо е провеждането на тестове и сканирания на мрежата за уязвимости и слабости от „потребители“ на Училищната компютърна мрежа след изричното уведомление и съгласуване с „отговорника по сигурността“.

е) Справяне с инциденти

- всеки „потребител“ или „отговорник по администрирането“ е длъжен да уведоми „отговорника по сигурността“ при установяване на инцидент със сигурността на услуга/мрежа или при съмнения за такъв.;
- в зависимост от сложността и обхвата на инцидента „отговорника по сигурността“ има право да поиска съдействие от външни експерти в лицето на CERT България.

*Забележка: Всички действия, които могат да бъдат предприети се извършват с изричното уведомяване на собственика/отговорника на хардуерното/софтуерното оборудване или съответния „отговорник по прекия контрол“.*

f) Други изисквания

Правилата за „мрежови достъп“ се допълват и от други документи, включени в Политиката за мрежова и информационна сигурност в Училищната компютърна мрежа на ВВВУ „Георги Бенковски“.

### **III. Анализ на риска.**

При неспазване на изискванията на този документ съществува риск към сигурността на информацията. Този риск може да бъде разделен, както следва:

- а) Заразяване на мрежата със зловреден софтуер;
- б) Получаване на нерегламентиран достъп до информация/информационни системи (вътрешно ведомствени);
- в) Извършване на нерегламентирани действия, които ще нарушат конфиденциалността, целостта и достъпността на информацията.

Мерките, които могат да бъдат предприети в посока на минимизиране на риска, са:

- системно обучение на „потребители“;
- извършване на системен контрол от страна на „отговорниците по прекия контрол“;

- наблюдение на достъпа до мрежата с възможност за организиране на няколкократно автентификация и преустановяване на достъпа на нарушителите и докладването им по надлежния ред.

#### **IV. Преглед и поддържане на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване, за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи.

„Отговорникът по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприети мерки за сигурност на това ниво.

#### **V. Предоставяне на достъп.**

Предоставянето на достъп се извършва във връзка с подпомагане на изпълнението на служебните задължения на служителите от ВВВУ „Георги Бенковски“ или обучението на различните категории обучаеми.

Правото на достъп до услуга се определя от „отговорника по прекия контрол“ (административния ръководител на „потребителя/структурата“) и се заявява в служба „КИС“.

#### **В „Заявката“ се посочват:**

- а) Организационна структура;
- б) Основание за предоставяне на достъп до услугата – определя се от „отговорника по прекия контрол“;
- в) Работни помещения/сграда, в които се предоставя достъпа.

#### **За служителя (обучаемия), на когото се предоставя достъп:**

1. Име, презиме и фамилия на „потребителя“, на който се предоставя достъп до услуга;
2. Длъжност на „потребителя“ (факултетен номер за обучаемите)

3. Организационна структура, към която принадлежи „потребителя“
4. Телефонен номер (вътрешен или ISDN телефонен номер) на „потребителя“
5. Наименование/тип на услугата
6. Други

**Забележка:** *В случаите, в които е необходимо и осигуряване на достъп до интернет, за осигуряване на служителите (обучаемите) се изпълняват изискванията на Приложение № 4 от настоящата политика („Организация на достъпа до интернет“).*

В случаи, при които се изгражда информационна среда без достъп до интернет, към гореспоменатата заявка се представя и списък на служителите (обучаемите), които е необходимо да бъдат включени.

**Списъкът трябва да съдържа информация за:**

1. Име, презиме и фамилия на служителя (обучаемия)
2. Длъжност на служителя (факултетен номер на обучаемия)
3. Работни помещения на служителя
4. Телефонен номер (вътрешен или ISDN телефонен номер) на служителя
5. Инвентарен номер на техническото средство (компютър, принтер, таблет и др.)
6. Регистрационен номер на носителя на информация за многократен запис (твърд или друг вид дисков носител) на техническото средство (ако разполага с такъв носител на информация)
7. Друга пояснителна информация

**VI. Преустановяване на достъп.**

Преустановяването на достъп до услуга може да се извърши в един от следните случаи и след подаване на заявка:

5. При преустановяване на трудовите/служебните правоотношения – пенсиониране, , уволнение и др.;

6. Доброволно – при нежелание от страна на „потребителя“ да продължи да използва предоставения му достъп до информационни системи, услуги и/или мрежи във връзка с изпълнението на служебните му задължения;

7. Принудително – извършва се от „отговорника по администрирането“ при следните случаи:

- едностранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа, до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **ЗНАЧИТЕЛНИ** вреди на служители, структури, информационни системи и услуги, собственост на ВВВУ „Георги Бенковски“. При този случай „отговорника по администрирането“ има право едностранно да прекрати достъпа до услугата;

- двустранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **НЕЗНАЧИТЕЛНИ** вреда на служители, структури, информационни системи и услуги собственост на ВВВУ „Георги Бенковски“ При този случай „отговорника по администрирането“ информира „потребителя“ за инцидента, размера на вредите, количеството необходимо време за възстановяване/отстраняване на проблема и др. След отстраняване на проблема, достъпа на „потребителя“ до услугата се възстановява;

8. други – всяко непредвидено обстоятелство, при което няма пряка заплаха за сигурността, но достъпа на „потребителя“ до предоставяната услуга е възпрепятстван (подмяна на офис техника, временна и/или постоянна неработоспособност на същата, хардуерни и/или софтуерни проблеми и др.).

**Забележка:** В случаи по т.1, т.2 и т.4 „потребителите“ са длъжни незабавно да уведомят „отговорника по администрирането“ и да осигурят достъп на

*същия до предоставената им офис техника с цел коректното ѝ изключване от УКМ (форматиране, презареждане със системен и приложен софтуер и др.) и последващото връщане на техниката.*

**Забележка:** *В случаи по т.3 „Отговорника по администрирането“ съгласува своите действия с „отговорника по сигурността“. Всеки инцидент се документира подробно и се предоставя на „собственика“ – т.5 от Приложение 6 към чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“.*

## **VII. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до Училищната компютърна мрежа и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** *В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция № И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.*

## ПРАВИЛА ЗА ОРГАНИЗАЦИЯ НА ДОСТЪПА ДО ИНТЕРНЕТ

### **Общи положения**

Този документ определя правилата за организация на „достъпа до Интернет“ на служителите и обучаемите във ВВВУ „Георги Бенковски“.

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите във ВВВУ „Георги Бенковски“ при организация на „достъп до Интернет“, при което да се запази конфиденциалността, целостта и достъпността до ресурсите на Училищната компютърна мрежа (УКМ) и се минимизира възможността на трети лица да получат неправомерен достъп до информационната инфраструктура.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“, които имат или желаят да получат достъп до Интернет, използвайки технически средства и мрежи на ВВВУ „Георги Бенковски“. На тези средства или мрежи **СЕ ЗАБРАНЯВА** създаване, обработване, съхранение и обмяна на класифицирана информация по смисъла на Закона за защита на класифицирана информация и правилника за прилагането му.

### **Обхват**

Правилата на настоящия документ се отнася за УКМ за обработване на „НЕКЛАСИФИЦИРАНА“ информация. Елементи на мрежата са изградени в административните, учебни и битови сгради на ВВВУ „Георги Бенковски“.

## **Собственик**

УКМ за достъп до Интернет е собственост на ВВВУ „Георги Бенковски“

### **I. Обща организация.**

Всички служители и обучаеми във ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

Свободното сърфиране в интернет и включването в други интернет дейности от страна на служителите и обучаемите във ВВВУ „Георги Бенковски“, не е привилегия.

Достъп до Интернет на служителите и обучаемите от ВВВУ „Георги Бенковски“ е допустимо само с използването на:

- изградената структурна кабелна система (СКС);
- мрежата за безжичен достъп (Wi-Fi мрежа);
- достъп до интернет през мобилни устройства (2G/3G/4G) – съгласно договори на ВВВУ „Георги Бенковски“ и Министерството на отбраната с обществени доставчици на мобилни услуги;

При осигуряването на „достъпа до Интернет“ в администрацията на ВВВУ, отговорностите на служителите могат да бъдат разпределени както следва:

#### **a) Собственик – ВВВУ „Георги Бенковски“;**

- осигурява необходимите финансови ресурси за поддръжка и управление на мрежата за достъп Интернет;
- делегира права за контрол на сигурността в мрежата;
- утвърждава настоящия документ.

#### **b) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

с) **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ - определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност

- определя се със заповед на началника на ВВВУ „Георги Бенковски“ като отговорник по мрежова и информационна сигурност в изпълнение на Наредбата за минималните изисквания за мрежова и информационна сигурност;

- има делегирани права за контрол на сигурността в мрежата за достъп до Интернет от „собственика“;

- отговаря за общото оперативно управление на сигурността на мрежата за достъп до Интернет;

- отговаря пряко за управлението на конфиденциалността, целостта и достъпността до информационните системи, услугите и мрежата;

- организира провеждане на тестове за откриване на уязвимости в информационните системи, услугите и мрежата;

- осъществява взаимодействие с CERT България при инциденти със сигурността;

- разработва и поддържа изискванията на настоящия документ;

- съвместно с „отговорника по администрирането“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата за достъп до Интернет;

- осъществява методическо ръководство по прилагане на изискванията на този документ.

d) **Отговорник по администрирането** - служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището;

- осъществява пряко управление на достъпа (включване/изключване) на „потребителите“ към мрежата за достъп до Интернет;

- осъществява пряко управление на трафичните капацитети за достъп до Интернет;

- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата;

- осъществява управлението на конфиденциалността, целостта и достъпността до информационните системи, услугите и мрежата;

- поддържа необходимата архитектура на мрежата за осигуряване на софтуерното осигуряване (системно и приложно) в актуално състояние;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата;

- участва в разработването и поддържането на изискванията на настоящия документ.

е) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- спазват изискванията на този документ;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата за достъп до Интернет.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълняват една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

## **II. Изисквания.**

### **Надеждност на информацията**

Цялата информация, която се получава от Интернет, трябва да се смята за подозрителна, освен ако не е потвърдена допълнително (електронен подпис или др.).

В тази връзка използването на информация от Интернет при изработване на официални документи, вземане на решения без тя да е допълнително проверена крие съответните рискове.

### **Проверка за вируси**

Всеки свален файл, независимо от размера и типа, трябва да бъде проверен с антивирусен софтуер.

**Забележка:** Препоръчително е файловете, които са „свалени“, преди отварянето им да бъдат проверявани с обновен с последни дефиниции антивирусен софтуер. Всяко отваряне на непроверени файлове крие съответните рискове за сигурността на информацията на „потребителя“, сигурността на ведомствените информационните системи и услуги и/или на мрежата като цяло.

### **Анонимност на потребителите**

**ЗАБРАНЯВА СЕ** погрешно представяне, анонимност, потискане или заменяне на идентичност на „потребители“ от мрежата за достъп до Интернет във ВВВУ „Георги Бенковски“ или в каквато и да е електронна комуникация. Всяка информация, която се публикува в публичното пространство трябва директно да рефлектира с действителния източник на информацията.

Допустимо е използване на анонимен достъп до информация при сваляне през FTP, UUCP, HTTP свързване и други.

## **III. Права и задължения.**

### **1. Осигуряване на достъп до Интернет.**

„Потребител“ на мрежата за достъп до Интернет на ВВВУ има право:

- да му бъде осигурен достъп до Интернет във връзка с изпълнението на служебните му задължения. Това право се определя от

административния ръководител на „потребителя“ и се заявява по установения ред;

- на квалифицирана помощ от „отговорника по администрирането“ във връзка с предоставеният му достъп до Интернет;

- да повишава своята професионална/езикова подготовка, използвайки предоставения им достъп до интернет;

- посещава интернет сайтове с информационен характер;

- посещават интернет сайтове от всякакъв характер, свързан с изпълнение на служебните му задължения и/или подобряващи тяхното изпълнение;

- да предоставя информация на „отговорника по администрирането“ за сайтове с пропаганден, противоконституционен, антисоциален, антидемократичен, с порнографски и/или педофилски характер, както и сайтове проповядващи религиозна омраза, дискриминация, призоваващи към извършване на престъпления и други подобни с цел ограничаването на достъпа;

- провеждат видео-конференции във връзка с лица и/или организации, с които ВВВУ „Георги Бенковски“ е партньор по силата на някакъв договор или споразумение. Тези конференции във връзка се изграждат във връзка с изпълнението на служебните задължения.

**Забележка:** Списъкът на разрешения софтуер е описан подробно в Приложение 5 – „Изисквания към базисната конфигурация (операционна система и софтуер) на персоналните работни места включени в УКМ.

На „потребителите“ на мрежата за достъп до Интернет на ВВВУ „Георги Бенковски“ се **ЗАБРАНЯВА:**

- Осъществяването на физическо включване/изключване на мрежови устройства и др. към ведомствената мрежа за достъп до Интернет, както и към мрежи на обществени телекомуникационни оператори за достъп до Интернет. Право да включва/изключва мрежови устройства към мрежата за достъп до Интернет има „отговорника по администрирането“;

- разпространение на информация, която може да компрометира сигурността на мрежата за достъп до Интернет, като потребителски имена и пароли, ключове за VPN, схеми, IP адресация, топология и др.;
- разпространение на нелицензиран софтуер, както и софтуер собственост на ВВВУ „Георги Бенковски“ (разработен или придобит чрез договори за доставка), както и софтуер предоставен от други организации или лица по силата на договорни отношения с тях;
- разпространение на материали, които са в противоречие със Закона за авторското право и сродните му права;
- осъществяване на достъп до нерегламентирани услуги;
- посещение на сайтове, които са пропагандни, противоконституционни, антисоциални, антидемократични, с порнографско съдържание и/или педофилия, проповядващи религиозна омраза, дискриминационни и други подобни, както и сайтове призоваващи към извършване на престъпления;
- промяна на целостта и конфигурацията на персоналните компютри и компютърната мрежа, към която са включени компютрите, в това число и включване на допълнително активно мрежово оборудване (маршрутизатори, комутатори, концентратори и др.) и/или предоставяне на достъп до услуги на допълнителни компютри, включени към допълнителни мрежови интерфейси;
- използване на софтуерни продукти, които „претоварват“ компютърната мрежа и/или услугите, както и създаващи неудобства или невъзможност за използване от други потребители. В това число спадат и слушането на „On-Line“ радиа и телевизионни канали, клипове и филми, освен ако това не е свързано пряко с изпълнението на служебните им задължения;
- използване на софтуерни продукти с цел придобиване на достъп над компютърни мрежи, персонални компютри, услуги или активно мрежово оборудване;
- използване на „peer-to-peer“ софтуерни продукти (torrent) с цел „сваляне“ или споделяне на файлове;

- използване на софтуерни продукти с цел предоставяне на отдалечен достъп до потребителите от ВВВУ „Георги Бенковски“, достъп на трети лица до компютри от локалната мрежа или споделяне на екрани. В това число спадат софтуерни продукти, като: TeamViewer, Skype, VNC, IP Vanish, PureVPN, Overplay, Hamachi, ExpressVPN и др. Изключения се допускат в следните случаи:

- при осигуряване на достъп на „отговорник по администрирането“ или администратор от друга организация, с цел поддръжка на придобит от тази организация хардуер или софтуер;

- за осигуряване на провеждането на учебен процес в условията на обстановка или обявено положение, при които се възпрепятства достъпа на обучаеми до територията на ВВВУ „Георги Бенковски“ за провеждане на нормален учебен процес;

- за осигуряване на изпълнението на функционалните задължения на служителите от ВВВУ „Георги Бенковски“, които по обективни причини са възпрепятствани от достъп до района на училището;

- за осигуряване на достъп до информационни услуги и ресурси, достъпа до които е организиран единствено през компютри от локалната мрежа на училището;

- други случаи, които могат да възникнат по повод изпълнението на функционални задължения, при които е невъзможно осигуряването на физически достъп на служителите или обучаемите до УКМ и в частно до мрежата с достъп до Интернет.

**Забележка:** при всички случаи отдалеченият достъп се осигурява при съгласуване с отговорника по прекия контрол, отговорника по сигурността и отговорника по администрирането.

- включване на класифицирани работни станции към неклассифицирани мрежи и/или интернет;

- използване/включване на класифицирани носители (твърди дискове, флаш памети, дискети) към неклассифицирани компютри.

## 2. Публично представяне.

### **„Потребителите“ ИМАТ ПРАВО:**

- да посочват своята принадлежност към ВВВУ „Георги Бенковски“ (списъци от електронни адреси, „chat“ сесии или други услуги);
- да изразяват позиция (тяхно лично мнение) по обществени въпроси;

### **На „потребителите“ е ЗАБРАНЕНО:**

- да изразяват мнение, при което се създава грешно впечатление, че е позиция на ВВВУ „Георги Бенковски“. Това включва: изявления от политически, расистки, полов, дискриминационен или друг подобен характер, както и публикуване на информация или съобщения, които могат да създадат конфликти или да породят негативна нагласа;
- да разкриват вътрешна информация чрез Интернет, като: информация, която може да повлияе на договори, връзки с трети лица, публично представяне на лица и организации и други.

**Забележка:** Публичното представяне на позицията на ВВВУ „Георги Бенковски“ се извършва от упълномощени лица. Техните права и задължения не са обект на настоящия документ.

## 3. Други изисквания.

Правилата за „достъп до Интернет“ се допълват и от други документи.

## **IV. Анализ на риска.**

Използването на Интернет от една страна подпомага служителите при изпълнението на служебните им задължения, но от друга страна крие и съответните рискове в следните аспекти:

1. Персоналния компютър/устройство от който потребителя упражнява предоставения му достъп до Интернет;
2. Мрежовата/информационната инфраструктура, към която е включен персоналния компютър/устройство;
3. Съхраняваната информация (лична и/или служебна);

4. Информационните системи и услуги (вътрешноведомствени и за публичен достъп).

Мерките, които могат да бъдат предприети в посока на минимизиране на риска, са:

- Спазването на изискванията настоящия и свързаните с него документи;
- Спазването на препоръките на „отговорника по администрирането“ и „отговорника по сигурността“;
- извършване на системен контрол от страна на „отговорниците по прекия контрол“;
- минимизиране на „безцелното сърфиране“ и безразборно „кликване“ по препратки към сайтове с неясен характер;
- наблюдение на достъпа до мрежа и изграждане на способности за откриване на „аномалии“ в мрежата;
- преустановяване на достъпа на нарушителите и докладването им по надлежния ред.

#### **V. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствени регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

#### **VI. Предоставяне на достъп.**

Предоставянето на достъп се извършва във връзка с подпомагане на изпълнението на служебните задължения на „потребителите“.

Достъпа до Интернет е персонален за „потребителите“ и се определя от „отговорника по прекия контрол“ (административния ръководител на „потребителя/структурата“). Той се заявява писмено чрез „Заявка за предоставяне на достъп до електронни услуги в мрежата за „НЕКЛАСИФИЦИРАНА“ информация на ВВВУ „Георги Бенковски“ (Приложение 13 от настоящите вътрешни правила или чрез друга утвърдена процедура), подписана от съответния „отговорник по прекия контрол“ и подадена до служба „Комуникационни и информационни системи“.

В „заявката“ се посочват:

1. Име, презиме и фамилия на „потребителя“, на който се предоставя достъпа до услугата;
2. Длъжност на „потребителя“;
3. Организационна структура, към която принадлежи „потребителя“;
4. Основание за предоставяне на достъп до услугата – определя се от „отговорника по прекия контрол“;
5. Работно помещение в което се предоставя достъпа;
6. Телефонен номер (вътрешен или ISDN телефонен номер) на „потребител“;
7. Инвентарен номер на техническото средство (компютър, принтер, таблет и др.);
8. Регистрационен номер на носителя на информация за многократен запис (твърд или друг вид дисков носител) на техническото средство (ако разполага с такъв носител на информация)
9. Наименование/тип на услугата;
10. Други;

## **VII. Преустановяване на достъп.**

Преустановяването на достъп до услуга може да се извърши в един от следните случаи:

1. При преустановяване на трудовите/служебните правоотношения – пенсиониране, преместване в други структури на министерството на отбраната, уволнение и др.;

2. Доброволно – при нежелание от страна на „потребителя“ да продължи да използва предоставения му достъп до информационни системи, услуги и/или мрежи във връзка с изпълнението на служебните му задължения;

3. Принудително – извършва се от „отговорника по администрирането“ при следните случаи:

- Едностранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа, до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **ЗНАЧИТЕЛНИ** вреди на служители, структури, информационни системи и услуги, собственост на ВВВУ „Георги Бенковски“. При този случай „отговорника по администрирането“ има право едностранно да прекрати достъпа до услугата;

- Двустранно - при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **НЕЗНАЧИТЕЛНИ** вреда на служители, структури, информационни системи и услуги собственост на ВВВУ „Георги Бенковски“. При този случай „отговорника по администрирането“ информира „потребителя“ за инцидента, размера на вредите, количеството необходимо време за възстановяване/отстраняване на проблема и др. След отстраняване на проблема, достъпа на „потребителя“ до услугата се възстановява;

4. Други – всяко непредвидено обстоятелство, при което няма пряка заплаха за сигурността, но достъпа на „потребителя“ до предоставяната услуга е възпрепятстван (подмяна на офис техника, временна и/или постоянна неработоспособност на същата, хардуерни и/или софтуерни проблеми и др.);

**Забележка:** В случаи по т.1, т.2 и т.4 „потребителите“ са длъжни незабавно да уведомят „отговорника по администрирането“ и да осигурят

достъп на същия до предоставената им офис техника с цел коректното ѝ изключване от УКМ (форматиране, презареждане със системен и приложен софтуер и др.) и последващото връщане на техниката.

**Забележка:** В случаи по т.3 „Отговорника по администрирането“ съгласува своите действия с „отговорника по сигурността“. Всеки инцидент се документира подробно и се предоставя на „собственика“ – от Приложение 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

### **VIII. Санкции.**

Всеки служител или обучаем във ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до Интернет и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция № И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

ИЗИСКВАНИЯ КЪМ БАЗОВАТА КОНФИГУРАЦИЯ  
(ОПЕРАЦИОННА СИСТЕМА И ПРИЛОЖЕН СОФТУЕР) НА  
ПЕРСОНАЛНИТЕ РАБОТНИ МЕСТА ВКЛЮЧЕНИ В УЧИЛИЩНАТА  
КОМПЮТЪРНА МРЕЖА (УКМ) НА ВВВУ „ГЕОРГИ БЕНКОВСКИ“

**Общи положения**

Този документ определя правилата по осигуряване на „базов системен/приложен софтуер“ на компютрите на служителите от ВВВУ „ГЕОРГИ БЕНКОВСКИ“.

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите от администрацията на ВВВУ при осигуряване на „базов системен/приложен софтуер“. Настоящите изисквания се налагат поради необходимостта от осигуряване на по-високо ниво на сигурност на УКМ, елиминиране на възможни колизии със закон за авторското право и сродните му права, други интелектуални права (извън договорените), или експортиране на контролиран софтуер и данни.

**Приложимост**

Изискванията на този документ важат за всички работещи (назначени по трудови или служебни правоотношения) в администрацията на ВВВУ „ГЕОРГИ БЕНКОВСКИ“, при което им е предоставен за използване персонален компютър във връзка с изпълнение на служебните им задължения.

Изискванията на настоящия документ определя необходимият „базов системен/приложен софтуер“ на компютрите, които са предназначени за създаване, обработване, съхранение и обмен на „**НЕКЛАСИФИЦИРАНА**“ информация по смисъла на Закона за защита на класифицирана информация и правилника за прилагането му.

Изискванията за „**базов системен/приложен софтуер**“ на персонални компютри, определени за работа с „**КЛАСИФИЦИРАНА**“ информация не са обект на настоящия документ.

### **Обхват**

Правилата на настоящия документ се отнасят за компютри, разположени в сгради от района на ВВВУ „ГЕОРГИ БЕНКОВСКИ“.

### **Собственик**

Материалните средства (персоналните компютри и периферия) са собственост на ВВВУ „ГЕОРГИ БЕНКОВСКИ“. Това право ВВВУ „Георги Бенковски“ упражнява чрез служба „Комуникационни и информационни системи“.

## **I. Обща организация.**

Всички служители от ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

### **а) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за закупуване и поддръжка на необходимият „базов системен/приложен софтуер“;
- делегира права за контрол;
- утвърждава настоящия документ.

### **б) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ;
- докладва на „отговорника по сигурността“ при неспазването на изискванията на този документ;

### **в) Отговорник за сигурността – съгласно чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“.**

- има делегирани права за контрол на сигурността от „собственика“;

- организира провеждане на тестове за откриване на уязвимости в „базов системен/приложен софтуер“, като при необходимост може да привлича външни експерти;

- разработва и поддържа изискванията на настоящия документ;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива;

- осъществява методическо ръководство по прилагане на изискванията на този документ;

- докладва на „отговорника по сигурността“ при неспазването на изискванията на този документ;

**d) Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- извършва инсталирането на „базовия системен/приложен софтуер“ на персоналните компютри на „потребителите“;

- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията;

- поддържат необходимата архитектура за осигуряване на „базовия системен/приложен софтуер“ в актуално състояние;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива;

- участва в разработването и поддържането на изискванията на настоящия документ;

- докладва на „отговорника по сигурността“ при неспазването на изискванията на този документ;

**e) Потребители** – всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“ са длъжни да:

- спазват изискванията на този документ;

- докладват на „отговорника по сигурността“ при компрометиране и съмнения за такива;

- докладват на „отговорника по сигурността“ при неспазването на изискванията на този документ

**Забележка:** Допустимо е служител(и) от ВВВУ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

## **II. Хардуерни параметри относно инсталацията.**

### **Твърд диск**

Независимо от капацитета се разделя на два дяла, както следва:

- Системен дял – от 60 до 200 GB (в зависимост от обема на твърдия диск);
- Потребителски дял – цялото останало налично пространство от твърдия диск.

## **III. Изисквания към операционната система.**

### **Операционна система**

Допустимите за използване операционни системи са:

- Microsoft Windows XP– по заявка, в съответствие с наличните лицензи за операционната система;
- Microsoft Windows 8.0 32/64 bit – по заявка, в съответствие с наличните лицензи за операционната система;
- Microsoft Windows 8.1 32/64 bit – по заявка, в съответствие с наличните лицензи за операционната система;
- Microsoft Windows 10 32/64 bit – по подразбиране;
- Linux 32/64 bit – по заявка.

### **Потребителски интерфейс**

Допустими езици на потребителския интерфейс на операционната система, както следва:

Английски – по подразбиране;

Български – по заявка. Настройва се при конфигуриране на персоналния компютър на работното място на потребителя.

### **Антивирусен софтуер**

Допустим за използване антивирусен софтуер, както следва:

- Microsoft System Center Endpoint Protection;
- Microsoft Windows Defender;
- Други антивирусни продукти – по заявка на потребителите и след утвърждаване от „отговорника по сигурността“.

### **Кирилизация**

Използват се стандартните, включени в дистрибуцията на операционната система, подредби:

- Фонетична подредба (Bulgarian (Phonetic Traditional)) – настройва се при конфигуриране на персоналния профил на потребителя;
- Стандартна BDS подредба (Bulgarian (Typewriter)) – настройва се при конфигуриране на персоналния профил на потребителя.

## **IV. Изисквания към приложния софтуер.**

### **Офис пакет**

Допустими за използване офис пакети, както следва:

- Microsoft Office 2016 32/64 bit
- Microsoft Office 2019 64 bit
- Microsoft Office 365
- OpenOffice – Windows и Linux версии;
- LibreOffice – Windows и Linux версии.

Минимален набор офис продукти включени в инсталацията:

- Microsoft Word 2016/2019 – по подразбиране;
- Microsoft Excel 2016/2019 – по подразбиране;
- Microsoft PowerPoint 2016/2019 – по подразбиране;

- Microsoft Outlook 2016/2019 – по подразбиране;
- OpenOffice Writer (Word Processor) – по заявка;
- OpenOffice Calc (SpreadSheet) – по заявка;
- OpenOffice Impress (Presentation) – по заявка;
- LibreOffice Writer (Word Processor) – по заявка;
- LibreOffice Calc (SpreadSheet) – по заявка;
- LibreOffice Impress (Presentation) – по заявка.

Допълнителни продукти от офис пакета, които могат да бъдат инсталирани:

- Microsoft Access (2016/2019) – по заявка;
- OpenOffice Base (Database Development) – по заявка;
- LibreOffice Base (Database Development) – по заявка;
- OpenOffice Draw (Drawing Program) – по заявка;
- LibreOffice Draw (Drawing Program) – по заявка;
- Microsoft Visio – по заявка, при налични лицензи за инсталация;
- Microsoft Project – по заявка, при налични лицензи за инсталация.

### **Софтуер за проверка на правопис**

Допустими езици за конфигуриране са:

- Английски език – по подразбиране;
- Български език – по подразбиране;
- Други езици – при наличие и по заявка.

### **Програми за разглеждане на страници в Internet/Intranet (Browser)**

Допустими за използване програми за разглеждане на страници в Internet, са както следва:

- Microsoft Internet Explorer/ Microsoft Edge – по подразбиране;
- Mozilla Firefox – по заявка;
- Opera – по заявка;
- Google Chrome – по заявка;

### Допълнителен софтуер

По подразбиране се инсталират софтуерни продукти към базовата система за поддръжка на:

- Portable Document Format (PDF) – Adobe Acrobat Reader или Foxit Reader;
- Архивни файлове – 7Zip;

По заявка и според наличните лицензи е допустимо инсталиране на друг софтуер, след одобрение от „отговорника по сигурността“.

### **V. Персонални настройки на потребителски профил.**

На персоналните компютри на потребителите допълнително се настройват:

- Настройки на принтер/скенер/плотер – по заявка.

### **VI. Сигурност.**

#### Парола на BIOS

Не се изисква.

#### Локален администратор

Изисквания:

- Име на администратора – Administrator - Променя се и е указан в “Регистър на работните станции”\*.
- Дължина на паролата – мин 8 символа;
- Изисквания за сложност/комплексност – всички основни групи символи и регистри;
- Права за разпространение на паролата – само за нуждите на „отговорниците за администрирането“. **ЗАБРАНЯВА СЕ** разпространение предоставените на „потребителите“ паролата/ите за достъп на трети лица.

*\*Забранява се промяната на зададената административна парола от неоторизирани лица.*

### Други потребители

Всички останали локални потребители се **ЗАБРАНЯВАТ**.

### Организационна принадлежност

Всички персонални компютри се присъединяват към изградената домейна организация „AF-ACAD.BG“, като:

- Общата политика за домейн „af-acad.bg“ се прилага към всички компютри;
- При създаването на потребители в домейн „AF-ACAD.BG“ в описанието на профила се добавя информация за: пълно име на потребителя, номер на стая, служебен телефонен номер, длъжност, организационна единица;

**ЗАБРАНЯВА** се предоставяне на административни права за достъп на „потребителите“, освен ако това не е свързано с изпълнение на служебните им задължения и за това не е информиран „отговорника по сигурността“. В този случай потребителят с отдаден административен достъп, придобива отговорност на “отговорник по администрирането”.

### Лицензи

Забранява се на всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“ да:

- разгласяват лицензни кодове за MS Windows;
- разгласяват лицензни кодове за MS Office пакети;
- разгласяват лицензни кодове за други продукти, предоставени им от ВВВУ „Георги Бенковски“.

### **VII. Други изисквания.**

„Потребителите“ **ИМАТ ПРАВО:**

- да му бъде осигурен персонален компютър, във връзка с изпълнението на служебните му задължения, инсталиран с „базов системен/приложен софтуер“. Това право се определя от административния ръководител на „потребителя“ и се заявява по установения ред;

- на квалифицирана помощ от „отговорника по администрирането“ във връзка с предоставеният му персонален компютър;
- да му бъде инсталиран допълнителен **„системен/приложен софтуер“** във връзка с изпълнението на служебните му задължения. Това право се определя от административния ръководител на „потребителя“ и се заявява по установения ред. Инсталирането на всеки необходим допълнителен системен/приложен софтуер, извън утвърдения списък, се съгласува с „отговорника по сигурността“. При наличието на минимален риск за сигурността на информационните системи, услугите, компютърната мрежа, персоналните компютри и информацията в тях, „отговорника по сигурността“ **ИМА ПРАВО да ЗАБРАНИ** използването на съответния софтуер. Практическата забрана се осъществява от „отговорника по администрирането“;

**Забележка:** Инсталирането на „базовият системен/приложен софтуер“ е изключително право и се осъществява единствено от „отговорниците по администрирането“.

#### **ЗАБРАНЯВА СЕ:**

- Инсталиране на каквито и да са софтуерни продукти извън посочените в този документ, освен ако за това няма писмена аргументация. Писмената аргументация се изготвя от „отговорника по прекия контрол“ и се утвърждава от „отговорника по сигурността“;
- Инсталиране на каквито и да са софтуерни продукти, с които се нарушава закона за авторското право и сродните му права или не застрашава сигурността на УКМ във ВВВУ „Георги Бенковски“ ;
- Включване на персонални компютри, съдържащи „КЛАСИФИЦИРАНА“ информация, към мрежата с достъп до Интернет с цел активиране на системен/приложен софтуер;

Правилата за „базовият системен/приложен софтуер“ се допълват и от други документи.

## **VIII. Анализ на риска.**

При неспазването на изискванията на този документ съществува риск към сигурността на информацията. Този риск може да бъде разделен както следва:

1. Заразяване на мрежата със зловреден софтуер;
2. Получаване на нерегламентиран достъп до информация /информационни системи (вътрешно ведомствени);
3. Извършване на нерегламентирани действия, които ще нарушат конфиденциалността, достъпността и целостта на информацията.

Мерките, които могат да бъдат предприети в посока на минимизиране на риска, са:

- системно обучение на „потребителите“;
- извършване на системен контрол от страна на „отговорниците по прекия контрол“ и „отговорниците по сигурността“;
- наблюдение на достъпа до мрежата с възможност за организиране на няколкократно автентификация и преустановяване на достъпа на нарушителите и докладването им по надлежния ред.

## **IX. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствени регламентиращи документи;

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

## **X. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен персонален компютър и не спазва изискванията на настоящия документ, е обект на

дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 6

ПРАВИЛА ЗА ОРГАНИЗИРАНЕ НА ДОСТЪПА ДО ИНТЕРНЕТ ПРИ  
ИЗПОЛЗВАНЕТО НА WI-FI МРЕЖАТА

## **Общи положения**

Този документ определя правилата за осигуряване на „Wi-Fi достъп“ на служителите и обучаемите от ВВВУ „Георги Бенковски“

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите от ВВВУ „Георги Бенковски“ при осигуряване/използването на „Wi-Fi достъп“, при което да се запази конфиденциалността, целостта и достъпността до информационните системи, услугите и информацията в мрежата и се минимизира възможността на трети лица да получат неправомерен достъп до информационната инфраструктура.

## **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“, които имат или желаят да получат достъп до Wi-Fi мрежите на Училищната компютърна мрежа на ВВВУ „Георги Бенковски“ (УКМ). На средствата за достъп или Wi-Fi мрежите **СЕ ЗАБРАНЯВА** създаване, обработване, съхранение и обмяна на **КЛАСИФИЦИРАНА** информация по смисъла на Закона за защита на класифицирана информация и правилника за прилагането му.

Компютърната мрежа, осигуряваща достъп до информационните системи и услуги на УКМ е собственост на ВВВУ „Георги Бенковски“.

Правилата от настоящия документ се отнасят за мрежата за обработване на „**НЕКЛАСИФИЦИРАНА**“ информация.

### **I. Терминология.**

- WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) – метод за защита на безжични мрежи с използване на WPA2 и допълнителен „Pre-Shared“ ключ за автентификация;
- Wi-Fi (Wireless Fidelity) – технология, която позволява на устройства да обменят данни използвайки радио сигнали. Основно се

използват честоти около 2.4 GHz и 5 GHz. Wi-Fi се базира на спецификациите от серията стандарти IEEE 802.11x.

## **II. Обща организация.**

Всички служители и обучаеми от ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

Свободното сърфиране в интернет и включването в други интернет дейности от страна на служителите и обучаемите от ВВВУ „Георги Бенковски“, използвайки мрежата за безжичен достъп не е привилегия.

При осигуряването на „Wi-Fi достъпа до Интернет“ във ВВВУ „Георги Бенковски“, отговорностите на служителите могат да бъдат разпределени както следва:

### **р) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за поддръжка и управление на мрежата за Wi-Fi достъп до Интернет;
- делегира права за контрол на сигурността в Wi-Fi мрежата
- утвърждава настоящия документ.

### **q) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

### **г) Отговорник по сигурността – съгласно чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“**

- определя се със заповед на началника на училището като отговорник по мрежова и информационна сигурност в изпълнение на Наредба за минималните изисквания за мрежова и информационна сигурност;
- има делегирани права за контрол на сигурността в Wi-Fi мрежата от „собственика“;
- отговаря за общото оперативно управление на сигурността на Wi-Fi мрежата;

- отговаря пряко за управлението на конфиденциалността, целостта и достъпността до информационните системи, услугите във Wi-Fi мрежата;
- организира провеждане на тестове за откриване на уязвимости в информационните системи, услугите във Wi-Fi мрежата;
- осъществява взаимодействие с CERT България при инциденти със сигурността;
- разработва и поддържа изискванията на настоящия документ;
- съвместно с „отговорника по администрирането“ разследва инциденти със сигурността на информацията в информационните системи, услугите във Wi-Fi мрежата;
- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационни системи, услуги във Wi-Fi мрежата;
- осъществява методическо ръководство по прилагане на изискванията на този документ.

s) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- осъществява пряко управлението на достъпа (включване/изключване) на „потребителите“ към Wi-Fi мрежата;
- осъществява пряко управление на трафичните капацитети във Wi-Fi мрежата;
- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията в информационните системи/услугите във Wi-Fi мрежата;
- осъществява управлението на конфиденциалността, целостта и достъпността до информационните системи/услугите във Wi-Fi мрежата;
- поддържат необходимата архитектура на мрежата за осигуряване на софтуерното осигуряване (системно и приложно) в актуално състояние;
- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи/услуги във Wi-Fi мрежата;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационни системи, услуги във Wi-Fi мрежата;

- участва в разработването и поддържането на изискванията на настоящия документ.

t) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- Спазват изискванията на настоящия документ;

- Докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата на УКМ.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

### **III. Типове безжични мрежи за достъп до УКМ.**

Мрежата за безжичен достъп до ресурси на УКМ и Интернет е изградена в учебните корпуси и административната зона, Планетариума, лекционните зали и спалните помещения на курсантите от Батальона за подготовка на курсанти. Изградени са следните типове мрежи:

- Мрежа с високо ниво на сигурност – на потребителите се налага автентификация при свързването. Използва се метод за сигурност WPA2-PSK (Wi-Fi Protected Access 2 - PreShared Key) и парола.

- Мрежа с ниско ниво на сигурност – мрежа без автентификация при свързването. Мрежата е с ограничение за използване в часовия диапазон от 07:00 часа до 17:00 часа.

### **IV. Технологична база.**

Оборудването, което може да бъде използвано за достъп до WiFi мрежата е:

- Преносими компютри;
- Таблети;

- „smart“ телефони.

**Забележка:** Допустимо е използването и на лични устройства за достъп при спазване на установените правила за внасянето и използването им на територията на ВВВУ „Георги Бенковски“.

#### **V. Групи потребители.**

Потребителите на Wi-Fi мрежата могат да бъдат разделени на следните основни групи:

- Служители на ВВВУ „Георги Бенковски“;
- Обучаеми във ВВВУ „Георги Бенковски“;
- Потребители тип „гости“ в района на ВВВУ „Георги Бенковски“.

#### **VI. Права за достъп до типовете безжични мрежи.**

Правото за достъп на потребителите до Wi-Fi мрежата се определя от принадлежността на потребителите към определена група, а именно:

- **До мрежа с високо ниво на сигурност** – всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“ и „гости“ на училището при особени обстоятелства, определени от „собственика“ на мрежата;

**Забележка:** „Отговорника по сигурността“ чрез „отговорника по администрирането“ си запазва правото за промяна на правата или временно преустановяване на достъпа до Wi-Fi мрежите при наличие на риск от компрометиране и/или необходимост от налагане на по-високо ниво на сигурност.

#### **VII. Права и задължения.**

Всички служители и обучаеми във ВВВУ „Георги Бенковски“ имат право на достъп до Wi-Fi мрежата.

В Wi-Fi мрежата е разрешено създаването, обработването и обменът на „НЕКЛАСИФИЦИРАНА“ информация.

Мрежата за Wi-Fi достъп може да бъде използвана за достъп до ресурси в Интернет, като изискванията, задълженията и отговорностите на потребителите и техните права за достъп до ресурси в Интернет са описани подробно в Приложение 3 (Организация на достъпа до Интернет) от настоящата вътрешни правила.

„Потребителите“ имат право:

- на квалифицирана помощ от „отговорника по администрирането“ във връзка с предоставеният му Wi-Fi достъп;
- да повишават своята професионална/езикова подготовка, използвайки предоставения им Wi-Fi достъп;
- да посещават сайтове от всякакъв характер, свързан с изпълнение на служебните им задължения и/или подобряващи тяхното изпълнение;
- да предоставят информация на „отговорника по администрирането“ за сайтове с пропаганден, противоконституционен, антисоциален, антидемократичен, с порнографско и/или педофилски характер, както и сайтове проповядващи религиозна омраза, дискриминация, призоваващи към извършване на престъпления и други подобни с цел ограничаването на достъпа.

**Забележка:** При използване на преносими компютри - списъкът на разрешения софтуер е описан подробно в Приложение 5 - „Изисквания към базисната конфигурация (операционна система и софтуер) на персоналните работни места включени в УКМ“.

На „потребителите“ се забранява;

- разпространение на информация, която може да компрометира сигурността на УКМ, като потребителски имена и пароли, ключове за VPN, схеми, IP адресация, топология и др.;
- разпространение на нелицензиран софтуер, както и софтуер собственост на ВВВУ „Георги Бенковски“ (разработен или придобит чрез договори за доставка), както и софтуер предоставен от други организации или лица по силата на договорни отношения с тях (в това число влизат лицензите

за Microsoft продуктите предоставени по договори на държавната администрация на Република България);

- разпространение на материали, които са в противоречие със Закона за авторското право и сродните му права;

- посещение на пропагандни, противоконституционни, антисоциални, антидемократични, с порнографско съдържание и/или педофилия, проповядващи религиозна омраза, дискриминационни и други подобни, както и сайтове призоваващи към извършване на престъпления. Право на потребителите е да предоставят информация за подобни сайтове с цел забраняване на достъпа до тях;

- използване на софтуерни продукти, които „претоварват“ безжичната мрежа и/или услугите, както и създаващи неудобства или невъзможност за използване от други потребители. В това число спадат и слушането на „On-Line“ радиа и телевизионни канали, клипове и филми, освен ако това не е свързано пряко с изпълнението на служебните им задължения;

- използване на софтуерни продукти с цел придобиване на достъп над компютърни мрежи, персонални компютри, услуги или активно мрежово оборудване;

- създаване, обработване и обмен на класифицирана информация по смисъла на Закон за защита на класифицираната информация; включване на класифицирани работни станции под какъвто и да е предлог към Wi-Fi мрежата;

- използване/включване на класифицирани носители (твърди дискове, флаш памети, дискети) под какъвто и да е предлог към устройства свързани към Wi-Fi мрежата;

- погрешно представяне, анонимност, потискане или заменяне на идентичност на потребители на Wi-Fi мрежата при достъпване на Интернет. Всяка информация, която се публикува в публичното пространство трябва директно да рефлектира с действителния източник на информацията;

- едновременното включване на устройства към ведомствената Wi-Fi мрежа и други мрежи.

Правилата за „Wi-Fi достъп“ се допълват и от други документи.

### **VIII. Наблюдение и отчетни файлове.**

- Действията на „потребителите“ във Wi-Fi мрежите са обект на контрол в режим 24/7;

- „Отговорникът по сигурността“ чрез „отговорника по администрирането“ си запазва правото да преустанови достъпа на определен „потребител“ и/или Wi-Fi мрежа при компрометиране, съмнения за компрометиране или при неспазване на изискванията на настоящия документ от страна на „потребителите“. Достъпа на съответния „потребител“ се възстановява след провеждане на разследване от страна на „отговорника по сигурността“ и „отговорника по администрирането“. За предприетите действия и резултатите от проведената проверка от страна на отговорните длъжностни лица се уведомява „отговорника по прекия контрол“;

- Право за извършване на анализ на Wi-Fi мрежите има „отговорника по администриране“. Параметрите на анализа се уточняват предварително с „отговорника по сигурността“.

Препоръки към отчетните файлове:

- Необходимо е записите в отчетните файлове да съдържат информация в необходимия минимален обем за: дата/част, тип услуга, вид услуга, състояние на сесията;
- Отчетните файлове се съхраняват на отделен информационен масив;
- Период за съхранение – не по-малко от 6 (шест месеца);
- Анализ на отчетни файлове – не по-малко от един път на месец;
- Анализ/контрол на оборудването – при необходимост. Може да се извърши и от други структури

### **IX. Анализ на риска.**

При използването на Wi-Fi мрежата съществува известен риск за част от информационната инфраструктура, респективно и към УКМ. Този риск може да бъде разделен на три основни типа:

- Външен риск;
- Вътрешен риск;
- Системен риск.

При външния риск опитите за компрометиране ще дойдат от вън. Атакуващия е с висока мотивираност и личен интерес. Цел на подобна атака биха били Wi-Fi мрежите с високо ниво на сигурност.

При мрежите с високо ниво на сигурност защитата се осигурява от неколнократна защита от вмешателства и като цяло вероятността за компрометиране е минимална.

Допълнителни мерки, които могат да бъдат предприети в тази посока са:

- Намаляване на срока на валидност на ключовете на VPN;
- Увеличаване на дължината на ключа;
- Системен анализ и наблюдение на мрежовата активност и отчетните файлове.

Интерес за атакуващия би представлявала възможността за получаване на неограничен достъп до публичните мрежи и/или интернет чрез компрометиране на потребителски профил. За минимизиране на възможностите е необходимо:

- Съкращаване на срока за валидност на потребителските профили;
- Използване на различни пароли при последващо създаване на идентични потребителски профили.

Външния риск е реален, но при изпълнение на допълнителните мерки за сигурност и приемлив.

При вътрешния риск заплахата се извършва с помощта на служител от администрацията. Предоставянето на вътрешна информация на атакуващ може да компрометира както Wi-Fi мрежата, така и елементи на УКМ.

Вероятността за случването на злонамерено действие е много малка, но с изключително тежки загуби за ВВВУ „Георги Бенковски“ при реализация.

Мерките, които могат да бъдат предприети в посока на минимизиране са:

- Разпределение на отговорността за управление, наблюдение и контрол на Wi-Fi инфраструктурата;
- Системно обучение на потребителите на Wi-Fi мрежите;
- Wi-Fi мрежата да се изгради с възможност за елиминиране на компрометирани елементи (потребителски профили, пароли, ключове за VPN).

Системен риск – той се идентифицира с възможността от системни грешки при администрирането на Wi-Fi инфраструктурата. Мерките, които могат да бъдат предприети с цел елиминиране и минимизиране на загубите при рисково събитие:

- Системен, периодичен анализ и тестване на конфигурациите на техническите средства;
- Редовен анализ на отчетните файлове с цел откриване на слабости при конфигурирането.

## **Х. Предоставяне на достъп.**

Служителите подават „Заявка за предоставяне на достъп до електронни услуги в мрежата за „НЕКЛАСИФИЦИРАНА“ информация на ВВВУ „Георги Бенковски“ (Приложение 13 от настоящата вътрешни правила) до началника на служба „Комуникационни и информационни системи“, подписана от „отговорника по прекия контрол“ (административния ръководител на „потребителя“).

В заявката се посочва:

- Три имена, звание на заявителя;
- Длъжност;
- Организационна единица;

- Телефон;
- За какъв период се иска достъпа до мрежата;
- Какви технически/софтуерни средства ще се използват (телефон, мобилен компютър, таблет, операционна система и др.).

## **XI. Преустановяване на достъп.**

Преустановяването на достъп до услуга може да се извърши в един от следните случаи:

9. При преустановяване на трудовите/служебните правоотношения – пенсиониране, , уволнение и др.;

10. Доброволно – при нежелание от страна на „потребителя“ да продължи да използва предоставения му достъп до информационни системи, услуги и/или мрежи във връзка с изпълнението на служебните му задължения;

11. Принудително – извършва се от „отговорника по администрирането“ при следните случаи:

- Еностранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа, до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **ЗНАЧИТЕЛНИ** вреди на служители, структури, информационни системи и услуги, собственост на ВВВУ „Георги Бенковски“. При този случай „отговорника по администрирането“ има право еностранно да прекрати достъпа до услугата;

- Двустранно – при компрометиране или съмнение за такова на сигурността на компютърна система, услуга и/или мрежа до която е предоставен достъп на „потребителя“, при което има вероятност за причиняване на **НЕЗНАЧИТЕЛНИ** вреда на служители, структури, информационни системи и услуги собственост на ВВВУ „Георги Бенковски“ При този случай „отговорника по администрирането“ информира „потребителя“ за инцидента, размера на вредите, количеството необходимо

време за възстановяване/отстраняване на проблема и др. След отстраняване на проблема, достъпа на „потребителя“ до услугата се възстановява;

12. Други – всяко непредвидено обстоятелство, при което няма пряка заплахата за сигурността, но достъпа на „потребителя“ до предоставяната услуга е възпрепятстван (подмяна на офис техника, временна и/или постоянна неработоспособност на същата, хардуерни и/или софтуерни проблеми и др.).

**Забележка:** В случаи по т.1, т.2 и т.4 „потребителите“ са длъжни незабавно да уведомят „отговорника по администрирането“ и да осигурят достъп на същия до предоставената им офис техника с цел коректното ѝ изключване от УКМ (форматиране, презареждане със системен и приложен софтуер и др.) и последващото връщане на техниката.

**Забележка:** В случаи по т.3 „Отговорника по администрирането“ съгласува своите действия с „отговорника по сигурността“. Всеки инцидент се документира подробно и се предоставя на „собственика“ – т.6 от Приложение 6 към чл. 3 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

## **ХII. Преглед и поддържане на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България, ведомствени регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

## **ХIII. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до УКМ и не спазва изискванията на настоящия документ, е обект на дисциплинарни

наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ **„КЛАСИФИЦИРАНА“** информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция № И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 7

## ПРАВИЛА ЗА „ЧИСТО РАБОТНО МЯСТО“

### **Общи положения**

Този документ определя общите аспекти по осигуряване на „чисто работно място“ от служителите във ВВВУ „Георги Бенковски“.

**Целта** на документа е да определи общите правила по осигуряване на **„чисто работно място“**, при което ще се минимизира възможността на трети лица да получат неправомерен достъп до служебна/чувствителна информация.

## **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“, на които е предоставен достъп до информационни системи, услуги, активно мрежово оборудване, защитни стени и комуникационни канали, осигуряващи информационния обмен в Училищната компютърна мрежа (УКМ) във ВВВУ „Георги Бенковски“..

**Забележка:** Изискванията на този документ важат за информационни системи, услуги, активно мрежово оборудване, защитни стени и комуникационни канали, осигуряващи информационния обмен в УКМ, в които се създава, обработва и обмена **„НЕКЛАСИФИЦИРАНА“** информация по смисъла на Закона за защита на класифицираната информация и правилника за неговото прилагане.

## **Собственик**

Информационните системи, услугите и активното мрежово оборудване, осигуряващи информационния обмен в УКМ, както и информацията която служителите създават, обработват и обменят във връзка с изпълнението на служебните си задължения е собственост на ВВВУ „Георги Бенковски“.

## **I. Обща организация.**

Всички служители от ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

### **а) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за закупуване, поддръжка и управление на УКМ;
- делегира права за контрол на сигурността в мрежата;
- утвърждава настоящия документ.

**б) Отговорник по прекия контрол – всеки ръководител на структура от ВВВУ „Георги Бенковски“**

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ;
- осъществява методическо ръководство по прилагане на изискванията на този документ;
- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията.

с) **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ – определен със заповед на началника на училището като отговорник по мрежова и информационна

- има делегирани права за контрол на сигурността в мрежата за достъп до Интернет от „собственика“;
- отговаря за изпълнението и спазването на изискванията, заложиени в този документ;
- съвместно с „отговорника по прекия контрол“ разследва инциденти със сигурността на информацията;
- приема сигнали от „потребителите“ при компрометиране и съмнения за компрометиране на информация и устройства.

д) **Отговорник по администрирането** - служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- предоставя на „потребителите“ пароли за достъп до системите от УКМ.

е) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- спазват изискванията на настоящия документ

**Забележка:** Допустимо е служител(и) на ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

## **II. Права и задължения.**

### **1. Всеки „потребител“, Е ДЛЪЖЕН:**

- Да осигурява сигурността на всяка служебна/чувствителна информация (хартиени копия/ оригинали, електронни документи) на работното си място за времето когато не присъства лично (краткосрочно и дългосрочно отсъствие от работното място/помещение);
  - Да заключват/ защитават персоналните компютри (desktop-и) с пароли, когато напускат работните помещения.
  - Да не се оставя на видно място записани потребителско име и парола;
  - Да съхраняват всяка служебна/ чувствителна информация (хартиени копия/оригинали, електронни документи) на определените места когато не присъства лично (краткосрочно и дългосрочно отсъствие от работното място/помещение);
  - Да осигуряват сигурността на преносимите компютри, таблети, smart телефони, устройства/средства за съхранение на данни (USB устройства, твърди дискове, CD/DVD дискове и др.) (това включва превантивна защита от кражба и/или достъп до информация от тях от трети лица);
  - Да съхранява предоставените му от „отговорник по администрирането“ пароли за достъп до различните системи от УКМ, като не допуска достъпа до тях от трети лица;
  - Да почиства своевременно работните дъски/табла (черни и/или бели), съдържащи служебна/чувствителна информация;
  - Да не оставят без надзор отпечатана информация/документи на принтерите/факс апаратите;
  - Да изключват (shutdown) персоналните компютри и принтерите в края на работния ден;
  - Да информират незабавно „отговорника по сигурността“ при намиране на оставени без надзор документи, технически носители на информация и устройства;

**Забележка:** Допустими са отклонения от изискванията на настоящия документ единствено за системи (информационни и комуникационни) работещи в режим 24/7. Всички отклонения от изискванията на настоящия документ се съгласуват с „отговорника по сигурността“ чрез „отговорника по прекия контрол“.

## 2. На „потребителите“ **СЕ ЗАБРАНЯВА:**

- Да оставят без надзор преносимите компютри, таблети, smart телефони, устройства/средства за съхранение на данни (USB устройства, твърди дискове, CD/DVD дискове и др.) и документи оригинали/копия. Всеки подобен случай може да доведе до злоумишлени действия на трети лица и да навреди както на ВВВУ „Георги Бенковски“, така и на отделни служители/лица и граждани;

- Заснемането на работни помещения, документи (оригинали/копия), работните плотове (desktop) на персоналните компютри, работни дъски (черни/бели) с фотоапарати, мобилни устройства и/или др.

## 3. Други изисквания.

Правилата за „чисто работно място“ се допълват и от други документи.

## **III. Анализ на риска.**

При неспазването на изискванията на този документ съществува риск към сигурността на информацията. Този риск може да бъде разделен на следните типове:

1. Външен риск – при него опитите за достъп до информация и системи на УКМ идват от трети лица, които не са служители и обучаеми във ВВВУ „Георги Бенковски“ (при посещение на външни за ВВВУ „Георги Бенковски“ лица и фирми при изпълнение на договорни отношения);

2. Вътрешен риск – при него опитите за достъп до информация и системи на УКМ идват от лица, които са служители на администрацията и обучаеми във ВВВУ „Георги Бенковски“;

3. Друг риск – при служебни командировки – преносимите компютри, таблети, smart телефони, устройства/средства за съхранение на данни и други

като: USB устройства, твърди дискове, CD/DVD дискове и др. могат да напускат пределите на административните сгради във ВВВУ „Георги Бенковски“. При такива случаи има голяма вероятност до тези устройства и средства за пренос на данни да имат достъп и трети лица, които не са служители и обучаеми във ВВВУ „Георги Бенковски“. По тази причина риска от компрометиране на информация и системи на УКМ е много висок.

Стриктното спазване на изискванията на този документ ще редуцира риска за сигурността на информацията във ВВВУ „Георги Бенковски“ до приемлив.

Мерките, които могат да бъдат предприети в посока на минимизиране на риска, са:

- системно обучение на „потребителите“;
- извършване на системен контрол от страна на „отговорниците по прекия контрол“.

#### **IV. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят изискванията за създаване, съхранение и използване на паролите на служителите за достъп до различни информационни системи и услуги.

#### **V. Санкции.**

Всеки служител и обучаем във ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до УКМ и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите.

Приложение 8

## ПРАВИЛА ЗА УПРАВЛЕНИЕ НА ПАРОЛИТЕ

### **Общи положения**

Този документ определя правилата за „управление на паролите“ за достъп на служителите и обучаемите във ВВВУ „Георги Бенковски“ до училищната компютърна мрежа (УКМ).

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите от ВВВУ „Георги Бенковски“ при **„управлението на паролите“**.

Правилата описани в този документ регламентират изискванията за създаване, съхранение и използване на паролите на служителите за достъп до

различни информационни системи. Използването на „силни“ пароли е предпоставка за съхранението на конфиденциалността, целостта и достъпността до информационните системи, услугите и информацията в УКМ и се минимизира възможността на трети лица да получат неправомерен достъп до информационната инфраструктура.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаемите във ВВВУ „Георги Бенковски“, на които във връзка с изпълнението на служебните задължения е създаден потребителски профил със съответната парола за достъп.

### **Обхват**

Правилата на настоящия документ се отнася за УКМ във ВВВУ „Георги Бенковски“ за обработване на „**НЕКЛАСИФИЦИРАНА**“ информация по смисъла на Закона за защита на класифицираната информация и правилника за прилагането му. Елементи на УКМ са изградени в административните, учебните и спалните сгради на ВВВУ „Георги Бенковски“.

### **Собственик**

УКМ за достъп до Интернет е собственост на ВВВУ „Георги Бенковски“.. На всеки служител от администрацията на ВВВУ „Георги Бенковски“ в обхвата на УКМ се предоставя персонален потребителски профил с парола за достъп до училищните информационни системи.

### **I. Общи изисквания.**

Достъпът до всички информационни системи, услуги в УКМ се извършва с потребителско име и парола.

#### **а) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за закупуване на необходимото оборудване за поддръжка и управление на паролите на „потребителите“;

- делегира права за контрол и управлението на паролите на потребителите;

- утвърждава настоящия документ.

b) **Отговорник по прекия контрол** – всеки ръководител на структура от ВВВУ „Георги Бенковски“

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

- **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ – определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност:

- има делегирани права за контрол и управлението на паролите на потребителите от „собственика“;
- разработва и поддържа изискванията на настоящия документ;
- съвместно с „отговорника по администрирането“ разследва инциденти;
- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на пароли на „потребители“;
- осъществява методическо ръководство по прилагане на изискванията на този документ.

c) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- осъществява пряко управление на достъпа (включване/ изключване) на „потребителите“ и осигуряването на паролите;
- съвместно с „отговорника по сигурността“ разследва инциденти;
- осъществява пряко контрол и управление на паролите на потребителите;
- поддържат необходимата архитектура за контрол и управление на паролите на „потребителите“;
- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на пароли;

- участва в разработването и поддържането на изискванията на настоящия документ.

d) **Потребители** - всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- спазват изискванията на този документ;

- докладват на „отговорника по сигурността“ при компрометиране и съмнения за такива на предоставените му пароли.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности, и вменените им допълнителни такива.

## **II. Изисквания към паролите.**

- Минимална дължина на паролата – 8 (осем) символа;
- Максимално време за валидност на паролата – 180 (сто и осемдесет) дни;
- Минимално време за валидност на паролата – 7 (седем) дни;
- Изисквания за сложност на паролата – паролата трябва да включва поне три от следните категории: малки и големи букви (на латиница), цифри и специални символи;
- Брой грешни опити за въвеждане на паролата – 5 (пет) опита. След последният опит потребителският профил се блокира;
- Време за блокиране на потребителски профил след поредица грешни опити – 10 (десет) минути;
- Време за нулиране на брояча за блокиране на акаунт - 10 (десет) минути;
- Невъзможност за използване на стари пароли при смяна – 6 (шест) пароли.

### Препоръки:

Паролата не трябва да бъде лесна за разгадаване, т.е. да не се асоциирана пряко с „потребителя“ (рождени дати, имена на близки, градове, телефонни номера и др.).

### **III. Права и задължения.**

Право за създаване/промяна на пароли/ключове за достъп до УКМ на ВВВУ „Георги Бенковски“ имат единствено съответните „отговорници за администрирането“;

Препоръчително е използването на различни потребителски профили с различни пароли в случаи, при които служител от ВВВУ „Георги Бенковски“ извършва администриране на повече системи.

Всеки „потребител“, **Е ДЛЪЖЕН:**

- да съхранява предоставените му от „отговорник по администрирането“ пароли/ключове за достъп до различните системи от УКМ, като не допуска достъпа до тях от трети лица;
- да изпълнява изискванията на настоящия документ.

**ЗАБРАНЯВА се:**

- Използването на потребителски профили за всекидневна употреба (от „отговорниците по администрирането“) за промяна/създаване на пароли/ключове за достъп до различните системи от УКМ на „потребителите“;
- Предоставянето на права и създаване/промяна на пароли за достъп до различните системи от УКМ на „потребители“, освен ако тава не е свързано с изпълнението на служебните им задължения;
- Предоставянето на паролите/ключовете за достъп на трети лица;
- Записване/съхранение на потребителски имена и пароли на общодостъпни места (под и над клавиатури, монитори, табла и др.);
- Съхранение на потребителски имена и пароли на технически и хартиени носители, както и изпращането им по електронна поща, SMS и др.

**„Отговорника по администрирането“ има право:**

- да преустанови достъпа „потребител“ (до отстраняване на проблема) при констатиране на нарушения от страна на „потребителя“ и/или неспазването на изискванията на настоящия документ;
- длъжен е да информира „отговорника по сигурността“ и съответния „отговорник по прекия контрол“ в случаи на нарушения и/или неспазване на изискванията на настоящия документ.

#### **Други изисквания**

Правилата за „**управление на паролите**“ се допълват и от други документи.

#### **IV. Анализ на риска.**

Потребителските профили и паролите са основното средство за удостоверяване на служителите от администрацията и обучаемите от ВВВУ „Георги Бенковски“ в УКМ.

Компрометирането на парола на определен потребител може да доведе до компрометиране на:

- информация на потребител и/или група от потребители;
- една или няколко информационни системи/услуги от УКМ;
- елементи на системата за защита на периметрите и/или транспортната среда на мрежата на УКМ;
- цялата УКМ.

За компрометирането на парола на потребителски профил атакуващият може да използва една от следните техники:

- **keystroke logging** – често наричана и **keylogging** е техника при която се записват натисканите клавиши на клавиатурата на компютъра (обикновено без знанието на потребителите);
- **sniffing** – **sniffer** е софтуерно приложение или устройство, което може да чете, наблюдава и прави копие на данните обменяни в компютърната мрежа. Ако информацията не е криптирана атакуващия има пълен достъп до данните;

- **dictionary attack** – техника за разбиване на ключ/парола или механизъм за автентификация чрез многократни опити за разпознаване на ключа/паролата от често използвани милиони възможни. За провеждането на атаката атакуващия използва предварително подготвена база с фрази, които ще бъдат използвани;

- **brute-force атака** – разновидност на dictionary атаката с тази разлика, че фразите се генерират по време на атаката;

- **социален инженеринг** – техника използвана от хакерите за придобиване на информация, която да използват за злонамерени действия;

- **фишинг (phishing)** - опит за измама, умишлена заблуда, с цел споделяне на данни за достъп до банкови сметки, онлайн разплащателни процесори, акаунти на доставчици на лицензирани услуги или софтуер, акаунти в онлайн магазини, лични профили, акаунти в социални медии и всякаква друга чувствителна информация

- **други** - последствията, които могат да настъпят след компрометиране на парола/ключ за достъп са:

- уронване на авторитета на определен служител, организационна структура и/или администрацията на ВВВУ „Георги Бенковски“ и/или МО и БА;

- пълно или частично спиране на отделни системи или цялата УКМ за неопределен период от време;

- кражба на информация;

- изнудване.

В някои от случаите на компрометиране на парола/ключ последствията могат да достигнат до компрометиране на сигурността на УКМ като цяло.

За минимизиране и елиминиране на риска от компрометиране на пароли е от изключително значение:

- спазването на изискванията на настоящия документ;

- своевременно инсталиране на системните обновления;

- своевременно уведомяване на съответните „отговорници по администрирането“ и/или „отговорника по сигурността“ при компрометиране или съмнение за такова.

Препоръчително е:

- честата смяна на паролата от всички „потребители“ и „отговорници по администрирането“;
- изграждане и поддържане на система за наблюдение и разпознаване на аномалии в мрежата;
- въвеждане на механизми за използване на пароли за еднократна употреба;
- въвеждане на механизми за многофакторна автентификация.

## **V. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят изискванията за създаване, съхранение и използване на паролите на служителите за достъп до различни информационни системи и услуги.

## **VI. Санкции.**

Всеки служител и обучаем във ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до УKM и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „**КЛАСИФИЦИРАНА**“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по

сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 9

## ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА ЕЛЕКТРОННА ПОЩА В ИНТЕРНЕТ

### **Общи положения**

Този документ определя правилата за „управление на паролите“ за достъп на служителите и обучаемите във ВВВУ „Георги Бенковски“ до училищната компютърна мрежа (УКМ).

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите от ВВВУ „Георги Бенковски“ при „управлението на паролите“.

Правилата описани в този документ регламентират изискванията за създаване, съхранение и използване на паролите на служителите за достъп до различни информационни системи. Използването на „силни“ пароли е предпоставка за съхранението на конфиденциалността, целостта и достъпността до информационните системи, услугите и информацията в УКМ и се минимизира възможността на трети лица да получат неправомерен достъп до информационната инфраструктура.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаемите във ВВВУ „Георги Бенковски“, на които във връзка с изпълнението на служебните задължения е създаден потребителски профил със съответната парола за достъп.

### **Обхват**

Правилата на настоящия документ се отнася за УКМ във ВВВУ „Георги Бенковски“ за обработване на „**НЕКЛАСИФИЦИРАНА**“ информация по смисъла на Закона за защита на класифицираната информация и правилника за прилагането му. Елементи на УКМ са изградени в административните, учебните и спалните сгради на ВВВУ „Георги Бенковски“.

### **Собственик**

УКМ за достъп до Интернет е собственост на ВВВУ „Георги Бенковски“.. На всеки служител от администрацията на ВВВУ „Георги Бенковски“ в обхвата на УКМ се предоставя персонален потребителски профил с парола за достъп до училищните информационни системи.

### **I. Общи изисквания.**

Достъпът до всички информационни системи, услуги в УКМ се извършва с потребителско име и парола.

е) **Собственик** – ВВВУ „Георги Бенковски“

- осигурява необходимите финансови ресурси за закупуване на необходимото оборудване за поддръжка и управление на паролите на „потребителите“;

- делегира права за контрол и управлението на паролите на потребителите;

- утвърждава настоящия документ.

f) **Отговорник по прекия контрол** – всеки ръководител на структура от ВВВУ „Георги Бенковски“

- отговаря за прилагането на изискванията на настоящия документ;

- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ.

- **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ – определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност:

- има делегирани права за контрол и управлението на паролите на потребителите от „собственика“;

- разработва и поддържа изискванията на настоящия документ;

- съвместно с „отговорника по администрирането“ разследва инциденти;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на пароли на „потребители“;

- осъществява методическо ръководство по прилагане на изискванията на този документ.

g) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- осъществява пряко управление на достъпа (включване/изключване) на „потребителите“ и осигуряването на паролите;

- съвместно с „отговорника по сигурността“ разследва инциденти;

- осъществява пряко контрол и управление на паролите на потребителите;

- поддържат необходимата архитектура за контрол и управление на паролите на „потребителите“;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на пароли;

- участва в разработването и поддържането на изискванията на настоящия документ.

h) **Потребители** - всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- спазват изискванията на този документ;

- докладват на „отговорника по сигурността“ при компрометиране и съмнения за такива на предоставените му пароли.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности, и вменените им допълнителни такива.

## **II. Изисквания към паролите**

- Минимална дължина на паролата – 8 (осем) символа;
- Максимално време за валидност на паролата – 180 (сто и осемдесет) дни;

- Минимално време за валидност на паролата – 7 (седем) дни;

- Изисквания за сложност на паролата – паролата трябва да включва поне три от следните категории: малки и големи букви (на латиница), цифри и специални символи;

- Брой грешни опити за въвеждане на паролата – 5 (пет) опита. След последният опит потребителският профил се блокира;

- Време за блокиране на потребителски профил след поредица грешни опити – 10 (десет) минути;

- Време за нулиране на брояча за блокиране на акаунт - 10 (десет) минути;

- Невъзможност за използване на стари пароли при смяна – 6 (шест) пароли.

Препоръки:

Паролата не трябва да бъде лесна за разгадаване, т.е. да не се асоциирана пряко с „потребителя“ (рождени дати, имена на близки, градове, телефонни номера и др.).

### **III. Права и задължения.**

Право за създаване/промяна на пароли/ключове за достъп до УКМ на ВВВУ „Георги Бенковски“ имат единствено съответните „отговорници за администрирането“;

Препоръчително е използването на различни потребителски профили с различни пароли в случаи, при които служител от ВВВУ „Георги Бенковски“ извършва администриране на повече системи.

#### **Всеки „потребител“, Е ДЛЪЖЕН:**

- да съхранява предоставените му от „отговорник по администрирането“ пароли/ключове за достъп до различните системи от УКМ, като не допуска достъпа до тях от трети лица;
- да изпълнява изискванията на настоящия документ.

#### **ЗАБРАНЯВА се:**

- Използването на потребителски профили за всекидневна употреба (от „отговорниците по администрирането“) за промяна/създаване на пароли/ключове за достъп до различните системи от УКМ на „потребителите“;
- Предоставянето на права и създаване/промяна на пароли за достъп до различните системи от УКМ на „потребители“, освен ако това не е свързано с изпълнението на служебните им задължения;
- Предоставянето на паролите/ключовете за достъп на трети лица;
- Записване/съхранение на потребителски имена и пароли на общодостъпни места (под и над клавиатури, монитори, табла и др.);
- Съхранение на потребителски имена и пароли на технически и хартиени носители, както и изпращането им по електронна поща, SMS и др.

#### **„Отговорника по администрирането“ има право:**

- да преустанови достъпа „потребител“ (до отстраняване на проблема) при констатиране на нарушения от страна на „потребителя“ и/или неспазването на изискванията на настоящия документ;
- длъжен е да информира „отговорника по сигурността“ и съответния „отговорник по прекия контрол“ в случаи на нарушения и/или неспазване на изискванията на настоящия документ.

### **Други изисквания**

Правилата за „**управление на паролите**“ се допълват и от други документи.

### **IV. Анализ на риска.**

Потребителските профили и паролите са основното средство за удостоверяване на служителите от администрацията и обучаемите от ВВВУ „Георги Бенковски“ в УКМ.

Компрометирането на парола на определен потребител може да доведе до компрометиране на:

- информация на потребител и/или група от потребители;
- една или няколко информационни системи/услуги от УКМ;
- елементи на системата за защита на периметрите и/или транспортната среда на мрежата на УКМ;
- цялата УКМ.

За компрометирането на парола на потребителски профил атакуващият може да използва една от следните техники:

- **keystroke logging** – често наричана и **keylogging** е техника при която се записват натисканите клавиши на клавиатурата на компютъра (обикновено без знанието на потребителите);
- **sniffing** – **sniffer** е софтуерно приложение или устройство, което може да чете, наблюдава и прави копие на данните обменяни в компютърната мрежа. Ако информацията не е криптирана атакуващия има пълен достъп до данните;

- **dictionary attack** – техника за разбиване на ключ/парола или механизъм за автентификация чрез многократни опити за разпознаване на ключа/паролата от често използвани милиони възможни. За провеждането на атаката атакуващия използва предварително подготвена база с фрази, които ще бъдат използвани;

- **brute-force атака** – разновидност на dictionary атаката с тази разлика, че фразите се генерират по време на атаката;

- **социален инженеринг** – техника използвана от хакерите за придобиване на информация, която да използват за злонамерени действия;

- **фишинг (phishing)** - опит за измама, умишлена заблуда, с цел споделяне на данни за достъп до банкови сметки, онлайн разплащателни процесори, акаунти на доставчици на лицензирани услуги или софтуер, акаунти в онлайн магазини, лични профили, акаунти в социални медии и всякаква друга чувствителна информация

- **други.**

Последствията, които могат да настъпят след компрометиране на парола/ключ за достъп са:

- уронване на авторитета на определен служител, организационна структура и/или администрацията на ВВВУ „Георги Бенковски“ и/или МО и БА;

- пълно или частично спиране на отделни системи или цялата УКМ за неопределен период от време;

- кражба на информация;

- изнудване.

В някои от случаите на компрометиране на парола/ключ последствията могат да достигнат до компрометиране на сигурността на УКМ като цяло.

За минимизиране и елиминиране на риска от компрометиране на пароли е от изключително значение:

- спазването на изискванията на настоящия документ;

- своевременно инсталиране на системните обновления;

- своевременно уведомяване на съответните „отговорници по администрирането“ и/или „отговорника по сигурността“ при компрометиране или съмнение за такова.

Препоръчително е:

- честата смяна на паролата от всички „потребители“ и „отговорници по администрирането“;
- изграждане и поддържане на система за наблюдение и разпознаване на аномалии в мрежата;
- въвеждане на механизми за използване на пароли за еднократна употреба;
- въвеждане на механизми за многофакторна автентификация.

#### **V. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят изискванията за създаване, съхранение и използване на паролите на служителите за достъп до различни информационни системи и услуги.

#### **VI. Санкции.**

Всеки служител и обучаем във ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения е предоставен достъп до УКМ и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „**КЛАСИФИЦИРАНА**“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по

сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 10

ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА ИНФОРМАЦИОННИ,  
КОМУНИКАЦИОННИ РЕСУРСИ И ОФИС ОБОРУДВАНЕ,  
СОБСТВЕНОСТ НА ВВВУ „ГЕОРГИ БЕНКОВСКИ“

**Основни положения.**

Настоящият документ определя общите правила, регулиращи употребата на офис оборудване, включително информационни системи, собственост на ВВВУ „Георги Бенковски“ от служителите и обучаемите.

Този документ важи за всички служители (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ, използващи административните сгради и учебни зали на ВВВУ „Георги Бенковски“.

Използването на държавно оборудване за представителни цели и други функции е предмет на допълнително споразумение, съгласно съществуващи договорености. При договаряне на такава употреба, тя се счита по-скоро за

оторизирана, отколкото за „лична” употреба на оборудването. Необходимо е допълнителните договорености да бъдат удостоверени с официални документи.

Използването на оборудване извън договореностите, се счита за „лично” и е обект на настоящите правила.

Тези правила установяват привилегии и допълнителни отговорности на служителите и обучаеми от ВВВУ „Георги Бенковски“ и ги третира като отговорни личности, които са ключа към това ръководството да стане по-отговорно към тях. Те позволяват на служителите и обучаемите да използват държавното офис оборудване за лични цели когато такава експлоатация включва минимални допълнителни разходи за ведомството, и се извършва в извън работно време, като не противоречи на целите или дейностите на ВВВУ „Георги Бенковски“ и не нарушава етичния кодекс.

Тези правила не отменят действащите закони или директиви, или политики на и ВВВУ „Георги Бенковски“ от по-високо ниво.

## **I. ТЕРМИНОЛОГИЯ.**

1. **Привилегия**, в контекста на настоящите правила, означава, че Ръководството на ВВМУ разширява възможността служителите и обучаемите да използват държавното офис оборудване за лични цели в усилията си да създаде по-отзивчива работна и учебна среда. Настоящата вътрешни правила, обаче, не дава правото за използване на държавното офис оборудване за неправителствени цели. Както и не дава право за модифициране на оборудването, включително инсталиране на личен софтуер или извършване на промени в конфигурацията и настройките.

2. **Държавно офис оборудване, включително информационни ресурси** включва, но не се ограничава до: персонални компютри заедно със съответните периферни устройства и софтуер, библиотечни ресурси, комуникационна техника, включително мобилни телефони, факс машини,

фотокопирни, офис консумативи, връзка и достъп до Интернет, електронна поща и други информационни ресурси.

3. **Минимален допълнителен разход** означава, че използването на държавна офис техника за лични нужди от служителите е ограничена до случаите, в които организацията вече е осигурила оборудването или услугите и използването им за лични нужди от служителите и обучаемите няма да доведе до допълнителни разходи за ВВВУ „Георги Бенковски“, освен за амортизация и поддръжка и малки количества електроенергия, мастило, тонер и хартия.

Пример за такъв минимален разход е копиране на няколко листа, отпечатване на няколко страници на принтер, нерегулярно изпращане на съобщения по електронната поща, или ограничено използване на достъп до Интернет за лични нужди.

4. **Извън работно време на служителя** означава времето, през което не се предполага служителят да извършва служебна дейност.

5. **Лична употреба** означава дейност, несвързана официално или по друг начин с изпълнението на служебните задължения. На служителите изрично се забранява използването на държавно офис оборудване за развиване на частен бизнес.

Примери за забранени дейности са използване на държавни компютърна техника и Интернет връзка за целите на частни услуги в сферата на туризма или инвестициите.

6. **Информационни ресурси** означава оборудване или свързани помежду си системи и подсистеми използвани за автоматично извличане, съхранение, обработка, управление, контрол, изобразяване, прехвърляне, обмен, или получаване на данни или информация.

## **II. Пълномощия.**

В общия случай, служителите могат да използват офис оборудването държавна собственост само за одобрени цели. Както бе споменато по-горе, ограничената употреба за лични цели на офис оборудване държавна

собственост от служителите през извън работно време се счита за „оторизирана експлоатация” на държавна собственост.

### **III. Правила.**

На служители на ВВВУ „Георги Бенковски“ се разрешава ограничено използване на офис оборудване държавна собственост за лични цели, ако използването не противоречи на официалната дейност и включва минимални допълнителни разходи на ведомството. Тази ограничена употреба на офис оборудване държавна собственост е възможна в извън работно време. Привилегията за използване на държавно офис оборудване за недържавни цели може да бъде преустановена или ограничена по всяко време от ръководството на училището.

Настоящите правила по никакъв начин не ограничават използването на държавното офис оборудване и информационни ресурси за оторизирани или официални дейности, свързани с изпълнението на служебните задължения.

#### **1. Специфично осигуряване при употребата на оборудване и консумативи.**

Използването на държавно офис оборудване за лични цели не трябва да води до загуба на продуктивност у служителя или да влияе на служебните му задължения. В допълнение, тази употреба може да поражда само минимални допълнителни разходи за ВВВУ „Георги Бенковски“ от следното естество:

- Разходи за комуникационна инфраструктура – разходи за телефон, телекомуникационен трафик и т.н.;
- Използване на консумативи с определени лимити хартия, мастило, тонер и т.н.;
- Обща амортизация на активите;
- Съхраняване на данни на съответните устройства;
- Въздействие върху мрежовия трафик при достъп до ресурси в Интернет.

Служителите имат право, на ограничено използване на държавно офис оборудване за проверка на лични инвестиции, за търсене на работа или за комуникация с организации за набиране на доброволци.

## **2. Неправилна употреба за лични цели.**

От служителите се очаква професионално поведение на работното място, както и въздържане от използването на държавно офис оборудване за неподходящи дейности. Злоупотребата или неподходящата употреба на държавно офис оборудване включват:

- Всякаква употреба за лични цели, която би могла да причини претоварване, закъснение, или възпрепятстване на услугите, осигурявани от система или оборудване – държавна собственост. Например достъп до видео, музикални или други файлове могат да влошат достъпа до мрежовите ресурси като цяло. „Push“ технологията, използвана за Интернет и други непрекъсваеми потоци от данни също биха намалили продуктивността на цялата мрежа и се считат за неподходяща употреба.

- Използването на държавни системи като основа или платформа за получаване на неоторизиран достъп до други системи.

- Създаването, копирането и разпространението на верижни писма или на други масови електронни съобщения независимо от характера на съдържанието им.

- Използването на държавно офис оборудване за незаконни, неподходящи, или обидни за колегите или обществеността дейности. Такива дейности включват, но не се ограничават до: думи на омраза, подигравателни материали на расова, верска, религиозна или полова основа, както свързани с националност, сексуална ориентация или инвалидност.

- Създаването, изтеглянето, разглеждането, съхранението, копирането или разпространяването на материали със сексуално съдържание.

- Създаването, изтеглянето, разглеждането, съхранението, копирането или разпространяването на материали свързани с незаконни

залагания, оръжия, терористични дейности, и всякакви незаконни или забранени със нормативен акт дейности.

- Използването за търговски цели, „платени“ дейности или други извънслужебни бизнес дейности (например: платени консултации, продажба или администриране на бизнес транзакции, продажба на стоки и услуги).

- Участие във външни дейности, свързани с увеличаване на капитала, с предлагането на продукт или услуга, с лобиране, или участието в забранени незаконни политически организации.

- Използването за изнасяне на информация на новинарски групи, бюлетини или публични форуми без да бъдат оторизирани за това. Такава дейност включва всякакви варианти на използване, които биха създали впечатлението, че служителят комуникира в качеството си на служител на ВВВУ „Георги Бенковски“ (освен в случаите, в които служителят е изрично оторизиран за това) или употреба в разрез с мисията или позицията на училището.

- Всяка употреба, която би довела до по-голям разход на финансови средства.

- Провеждане на разговори от мобилни или стационарни устройства, които противоречат на етичния кодекс, водят до загуба на продуктивност у други служители и/или водят до допълнителни финансови разходи за ведомството извън определените с допълнителни разпоредителни документи.

- Неоторизиран достъп, употреба, копиране, предаване или разпространение на контролирана информация, включително компютърен софтуер или данни, съдържащи защитена информация, материал, обект на авторско право, търговска марка, или други интелектуални права (извън договорените), или експортиране на контролиран софтуер и данни.

### **3. Правилно представяне.**

Отговорност на служителите, при използването на държавно офис оборудване за лични цели е, да не създават грешното впечатление, че действат в качеството си на служители или обучаеми от ВВВУ „Георги Бенковски“. Ако има предпоставки такава лична употреба да се интерпретира като служебна, то тогава служителят трябва да подготви необходимото опровержение.

Едно подходящо опровержение е: „Съдържанието на това съобщение е от личен характер и не е свързано с позицията ми на служител на ВВВУ „Георги Бенковски“.“

#### **4. Право на ползване на държавно офис оборудване, информационни и комуникационни ресурси.**

Правото на ползване на държавно офис оборудване, информационни и комуникационни ресурси се определя от заеманата длъжност. Всяка промяна и/или заявяване за тяхното използване се удостоверява с официални документи, утвърдени и съгласувани по надлежния ред.

#### **5. Запазване на конфиденциалност.**

Служителите нямат право, и не би трябвало да очакват, запазване на конфиденциалността при използването на офис оборудване – държавна собственост за лични цели независимо по кое време, включително при достъпа до Интернет и електронната поща. Ако служителите желаят да запазят конфиденциалността на личните си дела, трябва да избягват използването на държавна собственост като персоналния компютър, достъпа до Интернет или електронната поща. С използването на държавното офис оборудване, служителите се съгласяват с разгласяване на информация относно достъпването от тях информационни ресурси (интернет страници, услуги и приложения), обработената или предавана от тях информация.

С използването на държавно офис оборудване от служителите за лични цели, те дават съгласието си за мониторинг и запис, с или без причина, на достъпа до Интернет, използването на e-mail и т.н. Държавните

комуникационни ресурси трябва да се използват с разбирането, че използването им е несигурно в общия случай, не е лично и не остава анонимно.

Системните администратори използват инструменти за засичане на неподходяща и не по предназначение употреба.

Електронните комуникации могат да бъдат достъпни, в рамките на ВВВУ „Георги Бенковски“, за служителите, които имат нужда от такъв достъп във връзка с изпълнение на служебните си задължения.

Системните администратори имат достъп до всички информационни и комуникационни ресурси, произтичащи в изпълнение и само на техните служебни задължения.

#### **IV. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи.

#### **V. Санкции.**

Всеки служител и обучаем на ВВВУ „Георги Бенковски“, на който във връзка с изпълнение на служебните му задължения са предоставени информационни, комуникационни ресурси и офис оборудване, собственост на ВВВУ „Георги Бенковски“ и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, подвеждане под съдебна отговорност и/или търсене на материална отговорност за нанесените щети в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите

се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

Приложение 11

## ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА МОБИЛНИ УСТРОЙСТВА

### **Общи положения**

Този документ определя общите аспекти при използване на мобилни устройства при получаване на достъп до информационни системи и услуги на Училищната компютърна мрежа (УКМ) във ВВВУ „Георги Бенковски“.

**Целта** на документа е да определи общите правила по осигуряване на конфиденциалността, целостта и достъпността до предоставяните услуги, да защити потребителите и техните устройства, както и да осигури непрекъсваемостта на работните процеси.

**Необходимостта** от създаването на този документ се определя от факта, че използването на мобилните устройства не кореспондира с нивото на заплахите, което създава съответните рискове за сигурността на информацията и информационните системи и услуги на Училищната компютърна мрежа.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“, а също така и за всички външни потребители (консултанти, представители на фирми и/или организации с които ВВВУ „Георги Бенковски“ има договорни отношения, студенти, курсанти, курсисти, стажанти и др.), на които им е предоставен достъп до електронни услуги от Училищната компютърна мрежа чрез служебни или лични мобилни устройства.

#### **Собственик**

Предоставените във връзка с изпълнението на служебните задължения мобилни устройства са собственост на ВВВУ „Георги Бенковски“. Това право то упражнява чрез служба „Комуникационни и информационни системи и киберсигурност“.

#### **I. Терминология.**

**Мобилно устройство** – комуникационно устройство, което е достатъчно малко, преносимо в ръка, джоб или малка чанта, с необходимите запаси от електрическа енергия, способно да работи самостоятелно за определено време без зареждане и притежава необходимите хардуерни и софтуерни интерфейси, чрез които може да осъществява връзка с различни типове мрежи за обмен на данни, глас и видео. Такива устройства например са Pocket PC, iPhone, iPad, Smart телефони, BlackBerry, таблети и др.

#### **Общи изисквания**

Всички служители са длъжни да спазват наложените в този документ изисквания и препоръки.

##### **а) Собственик – ВВВУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за поддръжка и управление на мобилните устройства, чрез които се достъпват информационни ресурси на УКМ;
- делегира права за контрол и управление на мобилните устройства;
- утвърждава настоящия документ.

**b) Отговорник за сигурността** – съгласно чл. 3 от „Наредба за минималните изисквания за мрежова и информационна сигурност“

- създава, адаптира, променя и поддържа настоящите правила в актуално състояние;
- осъществява методическо ръководство по прилагане на този документ;
- отговарят за изпълнението и спазването на изискванията заложиени в този документ;
- съвместно с „отговорника по администриране“ разследва инциденти със сигурността на мобилни устройства;
- приема сигнали от „потребителите“ при компрометиране и съмнения за компрометиране на мобилни устройства;
- отговаря за документирането на процедури и инструкции, които се отнасят към този документ, както и поддържането на тяхното актуално състояние;
- осъществява посредничество с групите потребители и администратори, към които този документ се отнася.

**c) Отговорник по администрирането** – служител от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- отговаря за инсталирането, поддръжката и настройката на мобилните устройства;
- поддържа актуален списък на мобилните устройства в училището;
- отговаря за поддръжката на необходимите услуги, които се предоставят до мобилните устройства;
- отговаря за прилагането на настоящата вътрешни правила;
- подава заявки за промяна/адаптация на настоящата вътрешни правила до „отговорника за сигурността“;
- отговаря за обучението на групите потребители.

d) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- да са запознати, да разбират и да приемат за изпълнение изискванията на този документ;

- да спазват изискванията на този документ;

- да информира „отговорника за сигурност“ и/или „отговорника по администрирането“ при възникване на критични ситуации водещи до компрометиране на сигурността на информацията и/или съмнения за това.

## **II. Права и задължения.**

1. **Отговорности на „потребителите“** – те са длъжни във връзка с изпълнение на служебните си задължения да използват предоставените им мобилни устройства с висока отговорност за постигане на максимални резултати в интерес на ВВВУ „Георги Бенковски“, като:

- проверят внимателно вида, типа, правата за достъп, съдържанието и работоспособността на мобилните устройства, които им се предоставят за използване;

- пазят предоставените им мобилни устройства от кражба или загубване. „Потребителите“ носят финансова отговорност за загубено, откраднато мобилно устройство. Размерът на финансовата санкция се определя от друг документ, който не е част тази вътрешни правила;

- не съхраняват и обменят класифицирана информация, по смисъла на Закона за защита на класифицираната информация (ЗЗКИ), посредством мобилното устройство.

### **„Потребителите“ имат право:**

- на квалифицирана помощ от „отговорника по администрирането“ във връзка с предоставеното му мобилно устройство;

- да използват лични мобилни устройства за достъп до информационни системи и услуги на Училищната компютърна мрежа при спазване на изискванията на този документ;

- да повишават своята професионална/езикова подготовка, използвайки предоставеното им мобилно устройство.

## 2. „Отговорниците за администриране“ са длъжни:

- стриктно да прилагат и спазват изискванията на настоящия документ;
- съвместно с „отговорниците за сигурността“ да разработват и внедряват процедури и инструкции за използване на мобилни устройства;
- да поддържат актуален списък на мобилните устройства, получили достъп до информационни ресурси на УКМ.

## 3. Други изисквания.

Правилата за използване на мобилни устройства се допълват и от други документи.

## III. Физическа сигурност.

1. Физическа сигурност – в случай на загуба или кражба на мобилно устройство (служебно и/или лично на което е предоставено достъп до услуги на Училищната компютърна мрежа), „Потребителите“ незабавно уведомяват „отговорника по сигурността“ с цел предприемане на необходимите действия.

2. Шофиране – употребата на мобилни устройства по време на шофиране е **ЗАБРАНЕНО**. Шофьорите могат да използват мобилни устройства когато автомобила е паркиран и/или те са извън превозното средство. Служители, на които им се налага (във връзка с изпълнение на служебните задължения) да използват мобилни устройства докато шофират, трябва да използват допълнителни „HANDS-FREE“ устройства.

3. Пароли – препоръчително е мобилните устройства да бъдат защитени с пароли.

4. Отдалечено блокиране/премахване – препоръчително е „отговорниците по сигурността“ съвместно с „отговорниците по администриране“ да поддържат механизми за отдалечено блокиране/премахване на загубено или откраднатото устройство, както и при компрометиране на устройство. Тази способност позволява на

администрацията на ВВВУ „Георги Бенковски“ да противодейства на компрометиране на информация съхранена на мобилно устройство и/или информация до която потребителят е получил достъп чрез това устройството.

5. Използване на камера – при навлизането в зони на сигурност, в които се създава, обработва, съхранява и пренася КЛАСИФИЦИРАНА информация по смисъла на ЗЗКИ, потребителите са длъжни да изключват или забраняват камерите на мобилните устройства.

#### **Забранява се:**

- Включването на мобилните устройства към компютри/устройства, част от Училищната компютърна мрежа, мрежи за обработване на класифицирана информация по смисъла на ЗЗКИ и/или други, като преносители на данни (USB памети), с цел зараждане на батерии, синхронизиране с резервни копия и/или създаване на нови и др.;

- Оставяне на мобилни устройства (служебни или лични) без надзор;

- Разкриване на информация, кореспонденция и/или друго (от мобилните устройства) свързана с изпълнението на служебните задължения на служителите.

#### **IV. Сигурност на операционната система.**

1. **Firmware** – „Потребителите“ са задължени да предоставят служебните си мобилни устройства на „отговорниците по администрирането“ за обновяване на „firmware“ и/или промяна на настройките.

2. **Операционна система** - „Потребителите“ са задължени да предоставят служебните си мобилни устройства на „отговорниците по администрирането“ за обновяване на операционната система и/или промяна на настройките.

3. **Заздравяване** – при настройването на мобилните устройства „отговорниците по администрирането“ забраняват/премахват всички ненужни услуги (като: ftp клиенти, Internet file-share клиенти и др.).

4. **Антивирусен софтуер** – мобилните устройства трябва да имат инсталирана и настроена антивирусна програма със съответните дефиниции.

5. **Персонална защитна стена** – препоръчително е инсталирането и използването на защитна стена на мобилните устройства на потребителите.

**Забранява се:**

Промяна на установените настройки на мобилните устройства от всички „потребители“, както инсталирането/промяната/деинсталирането на допълнителен софтуер от/на мобилните устройства;

- Синхронизирането на мобилните устройства с други устройства;
- Обмяна, съхранение на файлове/данни на мобилните устройства с непотвърден източник.

**V. Вътрешни правила за сигурност на личните мрежи.**

1. Обмен на данни – „потребителите“ имат право да обменят данни чрез използване на Bluetooth/Infrared оборудване, при спазване на следните изисквания за сигурност:

- a. използване на „security mode 3“;
- b. обмена на информация да се извършва в защитени зони, с минимално отстояние 100 m от публични зони;
- c. обмена между устройствата да се извършва при използване на доверен „ключ“ между двамата кореспонденти.

2. отговорности на „потребителите“:

a. обмена на информация да се извършва единствено с мобилни устройства собственост на ВВВУ „Георги Бенковски“, и/или лични устройства одобрени от „отговорника по сигурността“;

b. да извършват обмена на информация чрез Bluetooth/Infrared оборудване на мобилните устройства като: пазят в тайна информация относно достъпа, паролите, криптографския ключ и оборудването;

c. да забранят Infrared оборудването при наличие на функциониращо Bluetooth оборудване;

d. да използват Bluetooth/Infrared оборудването на мобилните устройства за обмен на информация единствено когато е наложително. През останалото време оборудването трябва да бъде изключено или забранено за използване.

**Забранява се:**

- Използването на Bluetooth оборудване на мобилни устройства с версия на Bluetooth по-малка от „2.1“. Използването на мобилни устройства с версия на Bluetooth по-малка от „2.1“ се разрешава от „отговорника по сигурността“;

- Свързването/сдвояването на мобилни устройства посредством Bluetooth или Infrared на обществени места и с устройства, които не са подвластни на настоящия документ;

- Извършването на действия като:

- o Sniffing;

- o Device ID spoofing;

- o DoS attacks,

- o Всякакви други атаки към други Bluetooth или Infrared устройства;

- o Неоторизирана модификация на Bluetooth/Infrared устройства;

- o Използване на анонимни (anonymous) при свързване на Bluetooth/Infrared устройства.

**VI. Сигурност на данните.**

„Потребителите“ имат право да съхраняват лични данни при спазване на изискванията на „Правилата за използване на информационни, комуникационни ресурси и офис оборудване, собственост на ВВМУ“.

**Забранява се:**

- На мобилните устройства да се съхранява класифицирана информация по смисъла на ЗЗКИ и/или неклассифицирана информация, която може да доведе до имуществени и/или неимуществени вреди на лица или организации;

- На мобилните устройства да се съхраняват пароли, кодове, персонални идентификационна информация и др., която при попадане в трети лица да доведе до компрометиране на информационна система или услуга или да създаде предпоставки до неправомерен достъп до информация.

## **VII. Сигурност на достъпа до корпоративния мрежов ресурс.**

### **1. Използване на безжичен достъп – „Потребителите“ имат право:**

- Да използват мобилните си устройства за получаване на достъп до информационни ресурси на УКМ през мрежите за безжичен достъп на ВВВУ „Георги Бенковски“;

- Достъпа до мрежа за безжичен достъп трябва да бъде преустановен от „потребителите“ ако:

- не е наложително използването на безжичен достъп до информационни ресурси;

- когато устройството се свързва към компютър с цел, синхронизиране, създаване на резервно копие или възстановяване от такова;

- когато потребителя има съмнения, че използваното от него устройство е обект на нерегламентирани действия или има съмнения за компрометиране на мобилното устройство;

### **2. Синхронизиране, backup и restore – процесът трябва да бъде извършван в доверена среда от „отговорниците по администриране“.**

### **3. „Потребителите“ са длъжни своевременно да докладват на „отговорниците по сигурността“ при нередности, компрометиране или опити за компрометиране на мобилни устройства и/или информация от тях.**

#### **Забранява се:**

- обмен на пароли, кодове, персонална идентификационна информация, цифрови сертификати и други през мрежи за безжичен достъп;

- синхронизиране, backup и restore от неотторизирани лица на неотторизирани компютри или устройства;

## **VIII. Интернет сигурност**

Достъпа до Интернет ресурси от мобилни устройства трябва да е съобразен с изискванията дефинирани в „Правила за организация на достъпа до Интернет“, „Правила за използване на електронната поща в Интернет“ и „Правилата за използване на информационни, комуникационни ресурси и офис оборудване, собственост на ВВВУ“Георги Бенковски“ от настоящата вътрешни правила;

## **IX. Анализ на риска.**

При използването на мобилни устройства за достъп до информационни ресурси от УKM съществува риск за част от информационната инфраструктура, респективно и към УKM като цяло. Този риск може да бъде разделен на три основни типа:

- външен риск;
- вътрешен риск;
- системен риск.

При външният риск атакуващия е с висока мотивираност и личен интерес. Цел на тази атака могат да бъдат подложени всички мобилните устройства на „потребители“, които проявяват небрежност при използването им (например при използване на мобилните устройства в публични зони). Този риск може да бъде доведен до минимални нива, дори и елиминиран при спазването на изискванията на този документ, като:

- винаги да се използва VPN;
- намаляване на срока на валидност на ключовете на VPN;
- увеличаване на дължината на ключа;
- друго.

Външният риск е реален, но при изпълнение на допълнителните мерки за сигурност той е приемлив.

При вътрешният риск заплахата се извършва от или с помощта на служител от ВВВУ „Георги Бенковски“. Тук мотивираността на атакуващия

също може да се определи като висока. Предоставянето на вътрешна информация на атакуващ може да компрометира както WiFi мрежата, така и елементи на Училищната компютърна мрежа. Вероятността за случването на злонамерено действие е много малка, но при успешно реализиране може да доведе до тежки загуби в това число и компрометиране на служебна информация, информационна система/и или услуга/и.

Мерките, които могат да бъдат предприети в посока на минимизиране на риска са:

- разпределение на отговорността за управление, наблюдение и контрол на мобилните устройства в мрежата;
- системно обучение на потребителите използващи мобилни устройства.

Системен риск – той се идентифицира с възможността от системни грешки или неправилно настройване на мобилните устройства. Мерките, които могат да бъдат предприети с цел елиминиране и минимизиране на загубите при рисково събитие:

- системен, периодичен анализ и тестване на конфигурациите, техническите средства за защита на конфигурациите;
- редовен анализ на отчетните файлове;
- поддържане на актуално състояние на операционните системи, приложен софтуер и използваното оборудване, осигуряващо работата на мобилните устройства.

## **Х. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи;

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

## **XI. Санкции.**

Всеки служител и обучаем във ВВВУ “Георги Бенковски“, на който във връзка с изпълнението на служебните задължения е предоставено мобилно устройство и/или използва лично такова и не спазва изискванията на настоящата вътрешни правила е обект на дисциплинарни действия в това число и прекратяване на трудови или служебни правоотношения.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ“Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

## ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА ТЕХНИЧЕСКИ НОСИТЕЛИ/УСТРОЙСТВА, ЗА СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ

### **Общи положения**

Този документ определя общите аспекти по използване на технически носители/устройства за съхранение на данни от служителите на ВВВУ „Георги Бенковски“.

**Целта** на документа е да определи общите правила по използване на технически средства/устройства за съхранение на данни, при което да се минимизира възможността за неправомерен достъп до служебна/чувствителна информация, изтичането на служебна/чувствителна информация или нейното унищожение.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) в ВВВУ „Георги Бенковски“, на които във връзка с изпълнението на служебните им задължения са предоставени технически носители/устройства за съхранение на информация и тези носители/устройства са предназначени за съхранение на „НЕКЛАСИФИЦИРАНА“ информация по смисъла на ЗЗКИ и правилника за прилагането му.

**Забележка:** Изискванията на този документ важат при използването на технически носители/устройства за съхранение на данни на

компютри/системи елемент на „Училищната компютърна мрежа“ (УКМ) във ВВБУ „Георги Бенковски“.

### **Собственик**

Техническите носители/устройства за съхранение на информация, предоставени на служителите на ВВБУ „Георги Бенковски“ са собственост на ВВБУ „Георги Бенковски“.

### **Обхват**

Правилата на настоящия документ се отнася за мрежата за обработване на „НЕКЛАСИФИЦИРАНА“ информация. Елементи на мрежата са изградени в сградите на ВВБУ „Георги Бенковски“.

## **I. Терминология.**

**Технически носител за съхранение на информация** – такива са магнитните носители (дискети, ленти), магнито-оптични носители за данни, CD/DVD носители.

**Техническо устройство за съхранение на информация** – всяко USB устройство (твърд диск, flash памет), всички разновидности на SSD карти, мобилни устройства (телефони, таблети, електронни четци), смарт карти и др. на които може да се съхранява информация.

**Система от УКМ** – всеки компютър, сървър, принтер и/или устройство (част от УКМ), което има необходимия интерфейс/слот за присъединяване на технически носител/устройство за съхранение на информация.

## **II. Обща организация.**

Всички служители от ВВБУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

### **а) Собственик – ВВБУ „Георги Бенковски“**

- осигурява необходимите финансови ресурси за закупуването, поддръжката и управлението на технически носители/устройства за съхранение на информация;

- делегира права за контрол на сигурността в мрежата;

- утвърждава настоящия документ.

б) **Отговорник по прекия контрол** – всеки ръководител на структура от ВВВУ „Георги Бенковски“

- отговаря за прилагането на изискванията на настоящия документ;
- извършва контрол на подчинените му служители по изпълнението на изискванията на настоящия документ;
- осъществява методическо ръководство по прилагане на изискванията на този документ;
- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията;

в) **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ -определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност

- има делегирани права за контрол на сигурността в мрежата за достъп до Интернет от „собственика“;
- отговаря за изпълнението и спазването на изискванията, заложиени в този документ;
- съвместно с „отговорника по прекия контрол“ разследва инциденти със сигурността на информацията;
- разработва и поддържа изискванията на настоящия документ;
- приема сигнали от „потребителите“ при компрометиране и съмнения за компрометиране на информация и устройства;
- съвместно с „отговорника по администрирането“ поддържа изискванията на настоящия документ в актуално състояние.

г) **Отговорник по администрирането** – служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището

- подпомага потребителите (оказва техническа помощ при необходимост) при използването на технически носители/устройства за съхранение на информация;

- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията;

- съвместно с „отговорника по сигурността“ поддържа изискванията на настоящия документ в актуално състояние.

е) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“

- спазват изискванията на този документ;
- докладват на „отговорника по сигурността“ при компрометиране и съмнения за такива на технически носители на данни, както и при констатиране на нерегламентираното им използване.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълнява(т) една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности, и вменените им допълнителни такива.

### **III. Права и задължения.**

#### **1. Права на „потребителите“:**

- Всеки „потребител“ има право да получи технически носител(и)/устройство(а) за съхранение на информация във връзка с изпълнението на служебните си задължения. Това право се определя от административния ръководител на „потребителя“ и се заявява по установения ред;

- Всеки „потребител“ има право на квалифицирана помощ от „отговорника по администрирането“ във връзка с използването на технически носители/устройства за съхранение на информация;

#### **2. Всеки “потребител”, Е ДЛЪЖЕН:**

- да се запознае с изискванията на настоящия документ;
- да проверява с антивирусна програма техническия носител/устройство за съхранение на информация преди употреба/включване към УКМ;

- да осигурява сигурността на предоставените му технически носители/устройства за съхранение на информация (това включва защита от кражба, загубване и/или достъп на трети лица до техническите носители/устройства);

- да информира незабавно „отговорника по сигурността“ при намиране на технически носители/устройства за съхранение на информация;

**Забележка:** Допустими са отклонения от изискванията на настоящия документ единствено след съгласуване с отговорниците по сигурността и администрирането.

### 3. На „потребителите“ **СЕ ЗАБРАНЯВА:**

- да оставят без надзор технически носители/устройства за съхранение на информация;

- на технически носители/устройства, които са предназначени за употреба/включване към УКМ да се съхранява класифицирана информация, по смисъла на ЗЗКИ, както и информация разкриваща служебна тайна (договори, пароли, организация на мрежата, контакти с отговорни длъжностни лица или страни по договори и др.), която би довела до нанасяне на вреда на служители от училището или трети лица;

- употребата на технически носители/устройства за съхранение на информация по начин, който може да повреди техническите носители/устройствата или устройствата към които се включват;

- използването на лични технически носители/устройства за съхранение на служебна информация.

Изключения от последното правило се допускат в следните случаи:

- ВВВУ „Георги Бенковски“ като собственик на инфраструктурата не може да осигури достатъчен брой технически носители/устройства, отговарящи на нуждите на потребителите;

- Техническите носители/устройства се използват от обучаемите за съхранение и пренос на информация, свързана с осъществявания от тях учебен

процес, стига това да не е свързано със съхранение на „КЛАСИФИЦИРАНА“ информация;

- Назначените по трудови или служебни правоотношения имат възложени задължения, които изискват предварително създаване на документи извън ИТ инфраструктурата на ВВВУ „Георги Бенковски“, като разработване на лекции, задания за практически занятия и упражнения и др.

Изключенията се допускат единствено при информиране от страна на потребителя на отговорника по прекия контрол, отговорника по сигурността или отговорника по администрирането.

#### 4. Други изисквания.

Препоръчителни са:

- CD/DVD и магнито-оптични носители на данни да се съхраняват по начин осигуряващ тяхната UV защита (далеч от пряка слънчева светлина);
- магнитни технически носители (външни HDD, FDD и др.) да се съхраняват далеч от източници на електромагнитна енергия;
- при използването на устройства притежаващи подвижни механични елементи (например въртящи дискове в HDD, CD/DVD) трябва да бъдат надеждно закрепени и далеч от източници на вибрации;
- При наличие на механизъм за защита от запис на информация на технически носител/устройство, същият да бъде изключван само при реална необходимост от това;

**Забележка:** Неправилното съхранение на носителите може да доведе до физическа повреда и загуба на информация.

Правилата за използване на технически носители/устройства за съхранение на информация се допълват и от други документи.

#### **IV. Анализ на риска.**

Поради относително малкия размер на техническите носители/устройства за съхранение на информация те лесно могат да бъдат изнесени извън периметъра на зоната на отговорност, загубени и/или

откраднати. Това налага предприемането на допълнителни мерки за недопускане на изтичане на служебна/чувствителна информация, компрометирането на която може да нанесе вреда на ВВВУ „Георги Бенковски“, длъжностни лица от училището или трети лица и/или организации.

Друг основен риск за техническите носители/устройства за съхранение на информация е възможността лесно да бъдат заразени със зловреден софтуер. Това може да стане при използването/включването към компютри, които не са част от УКМ.

#### ***Мерки за намаляване на риска***

- провеждане на регулярни проверки от „отговорниците по сигурността“ по отношение спазването на изискванията на този документ;
- обучение на „потребителите“ относно правомерното използване на техническите носители/устройства, както и за рисковете, които крие неправомерното им използване;
- осъществяване на контрол от страна на „отговорниците по прекия контрол“ на подчинените им служители по отношение спазването на изискванията и препоръките на този документ;
- на компютрите/сървърите в УКМ да се използват единствено устройства, които са предоставени на „потребителите“ от администрацията на ВВВУ „Георги Бенковски“ във връзка с изпълнението на служебните им задължения;
- съхранение на техническите носители/устройства за съхранение на информация на специални места, като каси, заключени, без свободен достъп до тях;

#### **V. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване, за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените

регламентиращи документи; „Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

## **VI. Санкции.**

Всеки служител на ВВВУ „Георги Бенковски“, на който във връзка с изпълнението на служебните задължения е предоставено техническо средство/устройство на което може да се съхранява информация и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ **„КЛАСИФИЦИРАНА“** информация, „отговорника по сигурността“ и/или „отговорника по администрирането“ незабавно уведомява служителя по сигурността на информацията във ВВВУ „Георги Бенковски“ (Служба „Сигурност на информацията“). В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инструкция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, българската армия и структурите на подчинение на министъра на отбраната при инциденти.

## ЗАЯВКА

### ЗА ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО ЕЛЕКТРОННИ УСЛУГИ В МРЕЖАТА ЗА „НЕКЛАСИФИЦИРАНА“ ИНФОРМАЦИЯ НА ВВВУ „ГЕОРГИ БЕНКОВСКИ“

1. Данни на служителя: \_\_\_\_\_

(звание, име, презиме и фамилия)

\_\_\_\_\_

(длъжност)

\_\_\_\_\_

(служба, отделение, катедра)

Инв./Сер. номер на компютъра: \_\_\_\_\_ Сер. номер на носителя на  
информация: \_\_\_\_\_ стая: \_\_\_\_\_ телефон: \_\_\_\_\_

### ДЕКЛАРАЦИЯ:

Запознат съм, че **имам право:**

- да ми бъде осигурен достъп до информационни и комуникационни ресурси от Училищната компютърна мрежа (УКМ) на ВВВУ „Георги Бенковски“ във връзка с изпълнение на служебните ми задължения;
- на квалифицирана помощ от отговорните администратори във връзка с използването на информационните системи и услуги на Училищната компютърна мрежа;
- да използвам предоставената ми от ВВВУ „Георги Бенковски“ компютърна техника, офис оборудване и информационни ресурси за оторизирани или официални дейности, свързани с изпълнението на служебните ми задължения.

**Длъжен съм:**

- да спазвам изискванията на политика за мрежова и информационна сигурност в министерството на отбраната, структурите на пряко подчинение

на министъра на отбраната и българската армия утвърдена с МЗ ОХ-311/09.04.2020 г и свързаните с нея документи;

- да спазвам Правилник за използване на училищната мрежа на Висше военновъздушно училище „Георги Бенковски” ;
- да не допускам, чрез свои действия и/или бездействия, уронването на авторитета на отделни служители, структури и/или на администрацията на ВВВУ „Георги Бенковски“, както и сигурността на същите при използването на информационните системи и услуги на Училищната компютърна мрежа;
- да докладвам на отговорните за администриране служители за нередности при експлоатацията и/или сигурността на отделни елементи или на УКМ като цяло.

#### **Забранено ми е:**

- да създавам, обработвам, съхранявам и обменям КЛАСИФИЦИРАНА информация по смисъла на чл. 28 (1) от ЗЗКИ, както и класифицирана информация на държава партньор на Република България и/или НАТО/ЕС;
- да разгласявам информация за структурата, организацията, управлението, контрола и наблюдението на отделни информационни системи, компютърни мрежи и/или на УКМ като цяло;
- да променям хардуерната и софтуерната конфигурация на предоставената ми от администрацията на ВВВУ „Георги Бенковски“ компютърна и офис техника;
- Неоторизираното използване и/или опити за такова на информационни системи, ресурси и мрежи от УКМ.

Известно ми е, че всички мои действия подлежат на контрол и проверка от съответните специализирани органи по сигурността с цел опазването на държавната и служебна тайна.

В случай на неправомерно използване на предоставеното ми офис техника (компютър, принтер и др.) и достъп до информационни ресурси на

Училищната компютърна мрежа подлежа на дисциплинарни действия в това число и прекратяване на трудовите ми или служебни правоотношения.

Дата:

Служител:

\_\_\_\_.\_\_\_\_.202\_\_г.

\_\_\_\_\_/\_\_\_\_\_/

(подпис)

2. Да се осигури достъп до следните информационни услуги:

Интернет	<input type="checkbox"/> да	<input type="checkbox"/> не
Електронна поща/mail.af-acad.bg	<input type="checkbox"/> да	<input type="checkbox"/> не
Достъп до e-learning.af-acad.bg	<input type="checkbox"/> да	<input type="checkbox"/> не
Достъп до www.af-acad.bg	<input type="checkbox"/> да	<input type="checkbox"/> не
	<input type="checkbox"/> да	<input type="checkbox"/> не
	<input type="checkbox"/> да	<input type="checkbox"/> не

Основание: \_\_\_\_\_

\_\_\_\_\_

Допълнителни изисквания: \_\_\_\_\_

\_\_\_\_\_

Дата:

Началник на: \_\_\_\_\_

\_\_\_\_.\_\_\_\_.202\_\_г.

\_\_\_\_\_/\_\_\_\_\_/

(звание, подпис, име и фамилия)

3. Данни за техническите средства – попълва се от лицето, което изпълнява заявката след нейното утвърждаване

ПЕРСОНАЛЕН КОМПЮТЪР/		ИНВ/С. №:	
Операционна система:			
MAC адрес:		_:_:_:_:_:_:_	
Комутатор-порт:			
IP адрес:		Username:	
e-mail адрес:			

Дата:

\_. . 202 \_ г.

Отговорник по администрирането КИС:

\_\_\_\_\_ / \_\_\_\_\_ /

(звание, подпис, име и фамилия)

Дата:

\_. . 202 \_ г.

Администратор на информационни услуги:

\_\_\_\_\_ / \_\_\_\_\_ /

(звание, подпис, име и фамилия)

## ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА КОМПЮТЪРНИТЕ ЗАЛИ ВЪВ ВВВУ „ГЕОРГИ БЕНКОВСКИ“

### **Общи положения**

Този документ определя правилата за използване на компютърните зали във ВВВУ „Георги Бенковски“ от служители и обучаеми.

**Целта** на документа е да дефинира общите изисквания и отговорностите на служителите и обучаемите във ВВВУ „Георги Бенковски“ при използване на компютърните зали, при което да се запази конфиденциалността, целостта и достъпността до ресурсите на Училищната компютърна мрежа (УКМ) и се минимизира възможността на трети лица да получат неправомерен достъп до информационната инфраструктура.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“, които желаят да използват компютърните зали във ВВВУ „Георги Бенковски“. На компютърните системи и мрежи от тези зали **СЕ ЗАБРАНЯВА** създаване, обработване, съхранение и обмяна на класифицирана информация по смисъла на Закона за защита на класифицирана информация и правилника за прилагането му.

### **Обхват**

Правилата на настоящия документ се отнася за УКМ за обработване на „НЕКЛАСИФИЦИРАНА“ информация. Компютърните зали са изградени и могат да бъдат изградени нови в катедри, департамент, колеж, библиотека и други в административните, учебни и битови сгради на ВВВУ „Георги Бенковски“.

### **Собственик**

Компютърните зали са собственост на ВВВУ „Георги Бенковски“.

### **VIII. Основни положения.**

Всички служители и обучаеми във ВВВУ „Георги Бенковски“ са длъжни да спазват наложените в този документ изисквания и препоръки.

Компютърните зали са свързани към Училищната Компютърна Мрежа (УКМ), чрез която се получава достъп до:

- файловете сървъри на УКМ;
- Интернет.

Компютърните зали във ВВВУ „Георги Бенковски“ служат преди всичко за провеждане на учебни занятия по изучаваните дисциплини с ползване на компютри.

Обучаемите могат да провеждат в компютърните зали самостоятелна работа за:

- подготовка на упражнения, курсови и дипломни работи;
- разширяване на знанията и уменията си по информационни технологии;
- ползване на информационните ресурси на Интернет.

Учебните занятия в компютърните зали се провеждат съгласно утвърденото от началника на ВВВУ „Георги Бенковски“ семестриално разписание.

Самостоятелната работа на обучаемите в компютърните зали се провежда в рамките на установеното работно време по отделен за всяка компютърна зала график, съобразен със семестриалното разписание.

Право за самостоятелна работа в компютърните зали има всеки обучаем от ВВМУ, който е:

- законно регистриран като обучаем във ВВВУ „Георги Бенковски“;
- изявил желание за самостоятелна работа в компютърните зали.

При самостоятелна работа в компютърните зали обучаемият може да получава достъп до два вида ресурси:

- само до персоналния компютър, на който работи в момента;

- до персоналния компютър и до ресурсите на УКМ, включително до Интернет.

При осигуряването на използването на компютърните зали във ВВВУ „Георги Бенковски“, отговорностите на служителите могат да бъдат разпределени както следва:

f) **Собственик** – ВВВУ „Георги Бенковски“;

- осигурява необходимите финансови ресурси за поддръжка и управление на компютърните зали;

- делегира права за контрол на сигурността в компютърните зали;

- утвърждава настоящия документ.

g) **Отговорник по прекия контрол** – всеки ръководител на структура от ВВВУ „Георги Бенковски“, в която има изградена компютърна зала

- отговаря за прилагането на изискванията на настоящия документ;

- извършва контрол на подчинените му служители и обучаеми, в касаещия го обем, по изпълнението на изискванията на настоящия документ.

h) **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ – определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност;

- определя се със заповед на началника на ВВВУ „Георги Бенковски“ като отговорник по мрежова и информационна сигурност в изпълнение на Наредбата за оперативна съвместимост и информационна сигурност;

- има делегирани права за контрол на сигурността в компютърните зали;

- отговаря за общото оперативно управление на сигурността на мрежата в компютърните зали;

- разработва и поддържа изискванията на настоящия документ;

- съвместно с „отговорника по администрирането“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата;

- приема сигнали от „потребителите“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата в компютърните зали и в УКМ като цяло;

- осъществява методическо ръководство по прилагане на изискванията на този документ.

i) **Отговорник по администрирането** - служители от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището;

- осъществява пряко управление на компютърните системи в компютърните зали;

- съвместно с „отговорника по сигурността“ разследва инциденти със сигурността на информацията в информационните системи, услугите и мрежата;

- осъществява управлението на конфиденциалността, целостта и достъпността до информационните системи, услугите и мрежата;

- поддържат необходимата архитектура на мрежата за осигуряване на софтуерното осигуряване (системно и приложно) в актуално състояние;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата;

- участва в разработването и поддържането на изискванията на настоящия документ.

j) **Завеждащ компютърна зала** – служител от ВВВУ „Георги Бенковски“ от структурата, в която е създадена компютърната зала

- осъществява пряк контрол по използването на компютърната зала;

- съвместно с „отговорника по администрирането“ осигурява инсталирането на необходимия приложен и системен софтуер на компютърните системи, както и тяхното администриране;

- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата в компютърната зала;

к) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения) и обучаеми във ВВВУ „Георги Бенковски“;

- спазват изискванията на този документ;
- докладва на „отговорника по сигурността“ при компрометиране и съмнения за такива на информационни системи, услуги и мрежата.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълняват една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

## **IX. Организация на самостоятелната работа на обучаемите в компютърните зали.**

Самостоятелната работа на обучаемите се провежда по седмичен график за всяка от компютърните зали в зависимост от натовареността на залата съгласно утвърденото от началника на ВВВУ „Георги Бенковски“ семестриално разписание.

Графикът със свободни часове за провеждане на самостоятелна работа за следващата седмица се обявява най-късно в петък до 14:00 часа.

При наличие на много желаещи за провеждане на самостоятелна работа се въвежда ограничение на времето за заемане на едно работно място до 1 час.

За допускане до компютърна зала за провеждане на самостоятелна работа обучаемият представя на завеждащия компютърната зала своята курсантска (студентска) книжка или друг документ, удостоверяващ неговия статус.

Завеждащият компютърната зала отразява в дневник (регистър) началния и крайния час на използването на определено работно място в залата от конкретния обучаем.

## **X. Права и задължения.**

### **4. Потребители.**

Потребителят има право да ползва всички програмни, информационни и технически ресурси на съответното работно място в компютърната зала.

Потребителят, който е регистриран като потребител в УКМ има право да ползва и предоставените му ресурси на мрежата, включително и достъп до Интернет.

При работа в компютърната зала потребителят носи персонална отговорност за комплектацията, изправността и работоспособността на компютъра, с който работи.

При работа в компютърната зала потребителят е длъжен:

в началото на своята работа да провери комплектацията, изправността и работоспособността на компютъра и при откриване на нередности незабавно да съобщи за тях на провеждащия занятието или на завеждащия компютърната зала;

- да спазва изискванията на Вътрешни правилата за мрежова и информационна сигурност в УКМ;
- да работи внимателно и да пази техниката от физически повреди;
- да пази тишина и да не пречи на другите потребители в залата;
- да изтрива от диска на компютъра всички създадени от него файлове и папки в края на работата си.

Потребителят няма право:

- да влиза в компютърната зала без разрешение на преподавател или на завеждащия компютърната зала;
- да влиза в компютърната зала с обемисти чанти и сакове;
- да внася в компютърната зала хранителни продукти и напитки;
- да премества компютъра или отделни негови устройства от едно работно място на друго;
- да отваря компютъра или неговите устройства, освен в случаите когато това се извършва под контрола на преподавател във връзка с провеждане на учебно занятие;

- да изнася от компютърната зала компютър, устройство или друга част от работното място;
- да използва външни устройства за съхранение на данни без разрешение на завеждащия компютърната зала;
- да променя настройките на техническите параметри на компютъра чрез SETUP менюто, освен в случаите когато това се извършва под контрола на преподавател във връзка с провеждане на учебно занятие;
- да сменя антивирусните защиты на компютъра, освен в случаите когато това се извършва под контрола на преподавател във връзка с провеждане на учебно занятие;
- да променя мрежовите идентификационни и конфигурационни параметри на компютъра, освен в случаите когато това се извършва под контрола на преподавател във връзка с провеждане на учебно занятие;
- да променя разположението на файловете и папки върху диска, освен в случаите когато това се извършва под контрола на преподавател във връзка с провеждане на учебно занятие;
- да изтрива от диска програми, файлове и папки, които не са записани (създадени) от него;
- да рестартира компютъра при влизане в залата на проверяващо длъжностно лице.

При констатиране на нарушения по т. III.1 или на правилата, регламентирани от Вътрешни правилата за мрежова и информационна сигурност в УКМ, потребителят се лишава от правото самостоятелно да работи извън планираните учебни занятия и в зависимост от вида на нарушението му се налагат санкции съгласно Вътрешни правилата за мрежова и информационна сигурност в УКМ.

#### **5. Завеждащ компютърна зала.**

- Подготвя и обявява график за самостоятелна работа в компютърната зала;

- Допуска съгласно графика обучаеми до работните места в компютърната зала;
- Приема работното място от обучаемия при неговото напускане на залата;
- Следи за реда в залата и спазването от обучаемите на правилата за работа с компютърните системи;
- При констатиране на нарушение от страна на обучаем отстранява обучаемия от залата и отразява вида на нарушението;
- В края на работния ден проверява наличността и комплектацията на работните места в залата;
- Отразява възникналите повреди и неизправности в техническите и програмните средства на компютрите в дневник за неизправностите и заявка за отстраняването им от „отговорника по администрирането“.

## **XI. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствени регламентиращи документи.

„Отговорника по сигурността“ съвместно с „отговорника по администрирането“ определят подходящото ниво на сигурност и набора от предприетите мерки за сигурност на това ниво.

## **V. Санкции.**

Всеки служител или обучаем във ВВВУ „Георги Бенковски“, на който е предоставена възможност за използване на компютърна зала и не спазва изискванията на настоящия документ, е обект на дисциплинарни наказания, в това число и прекратяване на трудовото или служебното правоотношение.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорникът по сигурността“ и/или „отговорникът по администрирането“ незабавно уведомява/т служителя по

сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, Българската армия и структурите на подчинение на министъра на отбраната при инциденти.

## ПРАВИЛА ЗА ИЗПОЛЗВАНЕ НА ЛИЧНИ УСТРОЙСТВА

### **Общи положения**

Този документ определя общите аспекти при използване на лични устройства при получаване на достъп до информационни системи и услуги на Училищната компютърна мрежа (УКМ) във ВВВУ „Георги Бенковски“.

**Целта** на документа е да определи общите правила по осигуряване на конфиденциалността, целостта и достъпността до предоставяните услуги, да защити потребителите и техните устройства, както и да осигури непрекъсваемостта на работните процеси.

**Необходимостта** от създаването на този документ се определя от факта, че използването на лични устройства не кореспондира с нивото на заплахите, което създава съответните рискове за сигурността на информацията и информационните системи и услуги на УКМ.

### **Приложимост**

Този документ важи за всички работещи (назначени по трудови или служебни правоотношения) във ВВВУ „Георги Бенковски“, а също така и за всички външни потребители (консултанти, представители на фирми и/или организации с които ВВВУ „Георги Бенковски“ има договорни отношения, студенти, курсанти, курсисти, стажанти и др.), на които им е предоставен достъп до електронни услуги от УКМ чрез лични устройства.

### **Собственик**

Предоставените във връзка с изпълнението на служебните задължения лични устройства са собственост на съответния потребител. ВВВУ „Георги Бенковски“ упражнява правото си на собственик на УКМ, до която потребителите получават достъп чрез личните си устройства, чрез служба „Комуникационни и информационни системи“.

## **I. Терминология.**

**Лично устройство** – всяко едно комуникационно устройство, чрез което може да се осъществи достъп до информационните и мрежови ресурси на УКМ и което не е собственост на ВВВУ „Георги Бенковски“. Тези устройства притежават вътрешна (вградена) памет за съхранение на информация, а също така могат да използват различни комуникационни интерфейси за съхранение на информация върху външни носители на информация. Такива устройства например са персонални стационарни компютри, преносими компютри (лаптопи), планшети и др.

## **II. Общи изисквания.**

Всички служители/потребители са длъжни да спазват наложените в този документ изисквания и препоръки.

е) **Собственик на информационната инфраструктура за достъп** – ВВВУ „Георги Бенковски“:

- осигурява необходимите финансови ресурси за поддръжка и управление на УКМ;
- делегира права за контрол и управление на информационната инфраструктура;
- утвърждава настоящия документ.

ф) **Отговорник за сигурността** – служител от ВВВУ „Георги Бенковски“ – определен със заповед на началника на училището като отговорник по мрежова и информационна сигурност:

- създава, адаптира, променя и поддържа настоящите правила в актуално състояние;
- осъществява методическо ръководство по прилагане на този документ;
- отговарят за изпълнението и спазването на изискванията заложи в този документ;
- съвместно с „отговорника по администриране“ разследва инциденти

със сигурността на личните устройства, които могат да компрометират сигурността на УКМ или обменяната в нея информация;

- приема сигнали от „потребителите“ при компрометиране и съмнения за компрометиране на личните устройства;

- отговаря за документирането на процедури и инструкции, които се отнасят към този документ, както и поддържането на тяхното актуално състояние;

- осъществява посредничество с групите потребители и администратори, към които този документ се отнася.

**g) Отговорник по администрирането** – служител от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището:

- отговаря за поддръжката на необходимите услуги, които се предоставят до личните устройства;

- отговаря за прилагането на настоящата вътрешни правила;

- подава заявки за промяна/адаптация на настоящата вътрешни правила до „отговорника за сигурността“;

- отговаря за обучението/инструктажа на групите потребители.

**h) Отговорник по регистрирането на лични устройства** – служител от служба „Комуникационни и информационни системи“ или нещатни длъжностни лица, определени със заповед на началника на училището:

- приема заявленията, подадени от желаещите да ползват лични устройства за достъп до ресурсите на УКМ на ВВВУ „Георги Бенковски“ или за използването им на територията на ВВВУ „Георги Бенковски“;

- приема заявленията, подадени от потребителите за окончателно изнасяне и преустановяване на достъпа до ресурсите на УКМ на ВВВУ „Георги Бенковски“ или преустановяване на използването на тези устройства на територията на ВВВУ „Георги Бенковски“;

- води регистър на всички получени от него заявления и предоставя тази

информация на началника на служба „Комуникационни и информационни системи“;

- да проверява на всеки три месеца за наличие на нерегистрирани устройства в обхвата на неговата отговорност, както и за наличността на вече регистрираните;

- предоставя на потребителите стикер с текст „НЕКЛАСИФИЦИРАНО“.

i) **Потребители** – всички работещи (назначени по трудови или служебни правоотношения), обучаеми или гости на територията на ВВВУ „Георги Бенковски“, в която функционира УКМ:

- да са запознати, да разбират и да приемат за изпълнение изискванията на този документ;

- да спазват изискванията на този документ;

- да информира „отговорника за сигурност“ и/или „отговорника по администрирането“ при възникване на критични ситуации водещи до компрометиране на сигурността на информацията и/или съмнения за това.

**Забележка:** Допустимо е служител(и) от ВВВУ „Георги Бенковски“ да изпълняват една или повече от гореизброените роли в зависимост от техните функционални задължения и отговорности и вменените им допълнителни такива.

### **III. Права и задължения.**

• **Отговорности на „потребителите“** – те са длъжни във връзка с изпълнение на служебните си задължения да използват личните си устройства с висока отговорност за постигане на максимални резултати в интерес на ВВВУ „Георги Бенковски“, като не съхраняват и обменят класифицирана информация, по смисъла на Закона за защита на класифицираната информация (ЗЗКИ), посредством личното си устройство.

„Потребителите“ имат право:

• Да използват лични устройства за достъп до информационни системи и услуги на УКМ при спазване на изискванията на този документ;

- На квалифицирана помощ от „отговорника по администрирането“ във връзка с използването на личното си устройство за достъп до ресурсите на УКМ.

#### **4. „Отговорниците за администриране“ са длъжни:**

- Стриктно да прилагат и спазват изискванията на настоящия документ;

- Съвместно с „отговорниците за сигурността“ да разработват и внедряват процедури и инструкции за използване на лични устройства;

#### **5. „Отговорник по регистрирането на лични устройства“**

- Да поддържат актуален списък на личните устройства, получили достъп до информационни ресурси на УКМ.

#### **6. Други изисквания.**

Правилата за използване на лични устройства се допълват и от други документи.

### **IV. Срокове за подаване на заявления и предоставяне на достъп.**

6. Курсантите от рота за подготовка на курсанти подават писмени заявления по образец (приложение 16) до отговорника по регистрирането на лични устройства един път в годината, съобразено с графика за учебната година – до 15.09.

7. Курсистите във ВВВУ „Георги Бенковски“ подават писмени заявления по образец (приложение 16) до отговорника по регистрирането на лични устройства до три дни след началото на съответния курс.

8. Служителите по трудови или служебни правоотношения подават писмени заявления по образец (приложение 16) до отговорника по регистрирането на лични устройства при обоснована необходимост от използването на лично устройство на територията на ВВВУ „Георги Бенковски“.

#### **Забранява се:**

- Нерегламентираното използване на лични устройства на територията

на ВВВУ „Георги Бенковски“, особено за достъп до кабелната мрежа от ИТ инфраструктурата на училището.

#### **V. Изнасяне на личните устройства.**

6. Всички потребители, които са регистрирали свои лични устройства за използване на територията на ВВВУ „Георги Бенковски“ могат да ги изнасят ежедневно при условие, че това изнасяне е за кратък период от време, след който ще продължи използването на устройството на територията на училището, без да са променени негови технически характеристики, докато е било изнесено.

7. При необходимост от окончателно изнасяне на устройството (устройството няма да бъде използвано повече на територията на ВВВУ „Георги Бенковски“) се спазва следната процедура:

- До 10 дни преди окончателното изнасяне потребителят уведомява отговорника по регистрирането на лични устройства или началника на служба „Комуникационни и информационни системи“ за намеренията си, като декларира дата, към която желае да се осъществи самото окончателно изнасяне;

- За потребителите курсанти/курсисти се организира проверка за наличие на класифицирана информация на личните им устройства, която трябва да се осъществи до три дни преди датата на окончателно изнасяне. Проверката се осъществява съвместно от началника на служба „Комуникационни и информационни системи“ и началника на секция „Сигурност на информацията“ или определени от тях служители от съответните служби.;

- Началника на служба „Комуникационни и информационни системи“ отразява в регистъра на личните устройства датата, от която устройството вече не се използва за постоянен достъп до ресурсите на УКМ на ВВВУ „Георги Бенковски“ или на територията на училището.

#### **Забранява се:**

- Окончателното изнасяне на лични устройства, без да са информирани началника на служба „Комуникационни и информационни системи“ и началника на секцията „Сигурност на информацията“;

#### **VI. Регистър на личните устройства, използвани на територията на ВВУ „Георги Бенковски“.**

3. Началникът на служба „Комуникационни и информационни системи“ отговаря за воденето на регистър на всички лични устройства, използвани на територията на ВВУ „Георги Бенковски“, попадащи в обхвата на настоящата вътрешни правила.

4. Добавянето на информация към регистъра се осъществява след получаване на данни от отговорниците за регистриране на лични устройства.

5. На всеки регистриран потребител се издава стикер с допустимото ниво на обработвана информация, съгласно ЗЗКИ. Стикерът трябва да бъде залепен на самото устройство и да бъде достъпен за проверка за времето на използване на личното устройство на територията на ВВУ „Георги Бенковски“.

#### **VII. Сигурност на данните.**

„Потребителите“ имат право да съхраняват лични данни на своите устройства.

##### **Забранява се:**

- На личните устройства да се съхранява класифицирана информация по смисъла на ЗЗКИ и/или неклассифицирана информация, която може да доведе до имуществени и/или неимуществени вреди на лица или организации;
- На лични устройства да се съхраняват пароли, кодове, персонални идентификационна информация и др., която при попадане в трети лица да доведе до компрометиране на информационна система или услуга или да създаде предпоставки до неправомерен достъп до информация, свързани с дейността на ВВУ „Георги Бенковски“.

#### **VIII. Сигурност на достъпа до корпоративния мрежов ресурс.**

4. Използване на безжичен достъп – „Потребителите“ имат право:

- Да използват личните си устройства за получаване на достъп до информационни ресурси на УКМ през мрежите за безжичен достъп на ВВВУ „Георги Бенковски“;

- Достъпът до мрежа за безжичен достъп трябва да бъде преустановен от „потребителите“ ако:

- Не е наложително използването на безжичен достъп до информационни ресурси;

- Когато потребителят има съмнения, че използваното от него устройство е обект на нерегламентирани действия или има съмнения за компрометиране на личното устройство;

5. „Потребителите“ са длъжни своевременно да докладват на „отговорниците по сигурността“ при нередности, компрометиране или опити за компрометиране на личните устройства и/или информация от тях.

#### **IX. Интернет сигурност.**

Достъпа до Интернет ресурси от лични устройства трябва да е съобразен с изискванията дефинирани в „Правила за организация на достъпа до Интернет“, „Правила за използване на електронната поща в Интернет“ и „Правилата за използване на информационни, комуникационни ресурси и офис оборудване, собственост на ВВВУ „Георги Бенковски“ от настоящата вътрешни правила;

#### **X. Анализ на риска.**

При използването на лични устройства за достъп до информационни ресурси от УКМ съществува риск за част от информационната инфраструктура, респективно и към УКМ като цяло. Този риск може да бъде разделен на три основни типа:

- Външен риск;
- Вътрешен риск;
- Системен риск.

При външния риск атакуващият е с висока мотивираност и личен интерес. Цел на тази атака могат да бъдат подложени всички лични устройства на „потребители“, които проявяват небрежност при използването им (например при използване на личните устройства в публични зони). Този риск може да бъде доведен до минимални нива, дори и елиминиран при спазването на изискванията на този документ, като:

- винаги да се използва VPN;
- намаляване на срока на валидност на ключовете на VPN;
- увеличаване на дължината на ключа;
- друго.

Външния риск е реален, но при изпълнение на допълнителните мерки за сигурност той е приемлив.

При вътрешния риск заплахата се извършва от или с помощта на служител от ВВВУ „Георги Бенковски“. Тук мотивираността на атакуващия също може да се определи като висока. Предоставянето на вътрешна информация на атакуващ може да компрометира както WiFi мрежата, така и елементи на УКМ. Вероятността за случването на злонамерено действие е много малка, но при успешно реализиране може да доведе до тежки загуби, в това число и компрометиране на служебна информация, информационна система/и или услуга/и.

Мерките, които могат да бъдат предприети в посока на минимизиране на риска са:

- Разпределение на отговорността за управление, наблюдение и контрол на личните устройства в мрежата;
- Системно обучение на потребителите използващи лични устройства.

Системен риск – той се идентифицира с възможността от системни грешки или неправилно настройване на личните устройства. Мерките, които могат да бъдат предприети с цел елиминиране и минимизиране на загубите при рисково събитие:

- Системен, периодичен анализ и тестване на конфигурациите, техническите средства за защита на конфигурациите;
- Редовен анализ на отчетните файлове;
- Поддържане на актуално състояние на операционните системи, приложен софтуер и използваното оборудване, осигуряващо работата на личните устройства.

## **XI. Преглед и поддръжка на документа.**

Изискванията и препоръките на настоящия документ са обект на периодично обновяване, за да се осигури подходящо ниво на сигурност в съответствие със законите на Република България и ведомствените регламентиращи документи;

## **XII. Санкции.**

Всеки служител и обучаем във ВВВУ „Георги Бенковски“, на който във връзка с изпълнението на служебните задължения използва лични устройства за достъп до ресурсите на УКМ и не спазва изискванията на настоящата вътрешни правила, е обект на дисциплинарни действия, в това число и прекратяване на трудови или служебни правоотношения.

**Забележка:** В случай на инцидент със сигурността, засягащ „КЛАСИФИЦИРАНА“ информация, „отговорникът по сигурността“ и/или „отговорникът по администрирането“ незабавно уведомява/т служителя по сигурността на информацията във ВВВУ „Георги Бенковски“. В този случай процесите по констатиране, отчитане, обобщаване, контрол и предоставяне на информация за инцидентите се извършва съгласно Инstrukция №И-4/26.09.2007г. за дейността на командирите (началниците, ръководителите) от министерството на отбраната, Българската армия и структурите на подчинение на министъра на отбраната при инциденти.

ДО НАЧАЛНИКА НА ВВВУ „ГЕОРГИ БЕНКОВСКИ“  
БРИГАДЕН ГЕНЕРАЛ ЮЛИЯН РАДОЙСКИ

**М О Л Б А**

от: \_\_\_\_\_

(Звание, име, презиме и фамилия)

на длъжност: \_\_\_\_\_

ГОСПОДИН БРИГАДЕН ГЕНЕРАЛ,

Моля, за Вашето разрешение да използвам личен компютър в района на ВВВУ „Георги Бенковски“.

Декларирам, че съм запознат/а с Политиката за мрежова и информационна сигурност на Училищната компютърна мрежа на ВВВУ „Георги Бенковски“ и нося отговорност за неспазването ѝ.

Прилагам формуляр на конфигурацията на компютърната система.

\_\_\_ . \_\_\_ . 20 \_\_\_ г.

гр. Долна Митрополия

\_\_\_\_\_  
(звание, подпис, име и фамилия)

СЪГЛАСУВАНО:

# ОТГОВОРНИК ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

\_\_\_\_\_

(звание, подпис, име и фамилия)

\_\_ . \_\_ . 20 \_\_ г.

## ФОРМУЛЯР НА КОНФИГУРАЦИЯ НА КОМПЮТЪРНА СИСТЕМА

Марка, модел и тип на компютърната система: _____
Потребител на компютърната система: _____, моб.тел. _____ / звание, име, презиме, фамилия /
Място, където ще се съхранява компютърната система: корпус № _____, стая № _____

### Хардуерна конфигурация на системата

№	Елемент	Марка, модел, тип, сериен номер
1.	Дънна платка	
2.	Процесор	
3.	Памет	
4.	Мрежов адаптер	
5.	Видео адаптер	
6.	HDD	
7.	CD / DVD	
8.	FDD	
9.	Монитор	

10.	Принтер	
11.	Скенер	

---

/ звание, подпис, име и фамилия /

\_\_\_\_. \_\_\_\_ . 20\_\_ г.

Устройството е окончателно изнесено на дата \_\_\_\_\_. Проверката преди  
изнасяне е извършена от \_\_\_\_\_.

(звание, подпис, име и фамилия)