Система по управление сигурността на информацията	**НП**	**Версия 1**
НАРЪЧНИК НА ПОТРЕБИТЕЛЯ НА „ВЕТИС“		**Влиза в сила от:**
Българска агенция по безопасност на храните		

НАРЪЧНИК НА ПОТРЕБИТЕЛЯ НА ВетИС

За потребителите на ИИС „ВетИС“
в ЦУ на БАБХ и ОДБХ

	име, длъжност, структурно звено	дата	подпис
Изготвена от:	Веселина Ангелова-Манева, главен експерт ИКТ, дирекция ИСИС	2021	
Съгласувана от:	Група по управление, Протокол №2/04.02.21 г. Кристиян Бащавелов, директор дирекция ИСИС	2021	
Утвърдена от:	проф. Д-р Паскал Желязков, ДВМ, изпълнителен директор на БАБХ	2021	

✉ Гр. София, 1606, бул. ”Пенчо Славейков” № 15А
☎ +359 (0) 2 915 98 20, 🖷 +359 (0) 2 915 98 98, www.babh.government.bg

1. Цел

Компютърните информационни и комуникационни системи и мрежи, както и наличната информационна база са неразделна част от дейността на Българска агенция по безопасност на храните (БАБХ). Агенцията е вложила значителни човешки, материални и финансови ресурси за изграждането на тези системи.

Основна между тези системи е единната уеб-базирана национална информационна система за регистрация, идентификация, проследяване на движенията и контрола на здравния статус на животните, свързан с ветеринарномедицинската дейност на БАБХ – ИИС „ВетИС“.

Със заповед на Изпълнителния директор на БАБХ в Агенцията е внедрена Система за управление сигурността на информацията (СУСИ), изградена в съответствие с изискванията на БДС ISO/IEC 27001:2017 „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания“. С внедряването на СУСИ се цели:

а) защита на вложените в информационни и комуникационни системи и мрежи инвестиции;

б) гарантиране конфиденциалността, целостта и наличността на съдържащите се и обработвани в системите данни;

в) ограничаване на риска за дейността на БАБХ, свързана с използването на „ВетИС“;

г) стриктно съблюдаване на приложимите национални и европейски нормативни изискания, както и на договорните задължения;

д) опазване доброто име на БАБХ.

Настоящият Наръчник е базиран на изисквания, определени във вътрешната нормативна база на БАБХ и в документацията на внедрената в Агенцията СУСИ.

В документа се съдържат указания и изисквания към потребителите на „ВетИС“ за защита на въвежданите, обработвани и съхранявани в системата данни от нерегламентиран достъп, неправомерно променяне, заличаване или повреда.

2. Обхват

Определените в настоящия документ изисквания са приложими за всички групи потребители на ИИС „ВетИС“ от ЦУ на БАБХ и ОДБХ, определени със Заповед на изпълнителния директор на БАБХ № РД 11-2171/25.10.2017 г., изменена с РД 11-204/31.01.2018 г. и заповед №РД 11-986/08.06.2018 г. Всеки потребител носи лична отговорност за спазването им.

3. Свързани документи

3.1. Вътрешни правила за мрежова и информационна сигурност на БАБХ.

3.2. Вътрешни правила за използването на информационно-комуникационните ресурси на БАБХ.

3.3. Заявка за включване или промяна на достъпа в ИИС „Вет ИС“ (приложения № 1, 2 и 3 към Заповед № РД 11-2171/25.10.2017 г.).

3.4. Протокол за проведено обучение (приложение № 5 към Заповед № РД 11-2171/25.10.2017 г.).

3.5. Протокол за регистриране на потребител в ИИС „ВетИС“ (приложение №6 към заповед РД 11-2171/25.10.2017 г.).

3.6. Политика на БАБХ по сигурност на информацията.

3.7. Инструкция за администратора на ВетИС.

3.8. Инструкция за администратора Модул мляко.

3.9. Технологична инструкция за коригиране на данни във ВетИС, утвърдена със Заповед №РД 11-216/09.02.2016 г. на изпълнителния директор на БАБХ.

3.10. Заповед РД 11-184 от 2010 г. за дейностите по потребителски групи.

3.11. Инструкция за потребителя модул „Обработка на данните за племенните животни, родени в страната или от внос и породи“.

3.12. Ръководство за потребителя за идентификация на пчелните семейства във ВетИС.

3.13. Ръководство за потребителя Модул мляко.

3.14. Инструкция за оператора/потребителя ВетИС.

4. Правила за достъп до ИИС „ВетИС“

4.1. Предоставянето на достъп до ИИС „ВетИС“ се извършва по реда, описан в Заповед № РД 11-2171/25.10.2017 г. и последващите й изменения. С внедряването на СУСИ не настъпват промени в утвърдените правила за достъп до интегрирана информационна система и до поддържащата я инфраструктура.

4.2. Потребителите имат достъп до системата в рамките на дадените им права, съобразно потребителската група, към която са присъединени. Те следва да ползват „ВетИС“ ефективно, етично и законосъобразно, само за целите, за които им е осигурен достъп и в съответствие с осъществяваните от тях дейности, съгласно чл. 27, ал. 1. на Наредба № 6, издадена от министъра на земеделието и храните, последно изменение с бр. 5 на ДВ от 12.01.2018 г., в сила от 12.01.2018 г.

4.3. Предоставянето на достъп до „ВетИС“ се извършва след подаване по реда на Заповед № РД 11-2171/25.10.2017 г. на заявки (приложение 1, 2 или 3 от заповедта).

4.4. Конкретни инструкции се следват от администраторите на „ВетИС“ съгласно утвърдена вътрешна „Инструкция за администратора на ВетИС“.

4.5. Достъпът до „ВетИС“ е персонален. Потребителите нямат право да го предоставят на други лица.

4.6. Потребителите, създаващи информация, подлежаща на въвеждане в ИИС „ВетИС“, гарантират лично нейното качество, пълнота и достоверност.

4.7. Потребителите, въвеждащи данни в ИИС “ВетИС”, гарантират лично тяхното правилно вписване, качество, пълнота и достоверност.

4.8. При осъществяване на VPN връзка със системата, потребителите трябва да ползват устройства, имащи като минимум наличие на работеща антивирусна система с актуални дефиниции, работеща защитна стена и защита с парола на достъпа до устройството. Препоръчително е да има криптиране на ниво диск.

4.9. Потребител, който подозира, че работното му устройство е поразено от вирус, ТРЯБВА ВЕДНАГА ДА прекрати връзката с „ВетИС“, и незабавно да уведоми този, който му е предоставил правото на достъп (дирекция ИСИС към ЦУ на БАБХ или регионални администратори към ОДБХ), за да се предприемат неотложни и подходящи мерки за премахване на заразяването от устройството. В този случай, регионалният администратор следва незабавно да уведоми поддържащата фирма за предприемане на съответните действия. Задължително следва да се уведоми дирекция ИСИС при настъпили инциденти и събития.

4.10. Защитата на личната информация и данни, съхранявани и обработвани в БАБХ е гарантирана, както се изисква от Закона за защита на личните данни, други нормативни разпоредби и/или клаузи по договори. Прилагат се изискванията на внедрените процедури за обработка и защита на лични данни в БАБХ. Нормативните изисквания по отношение на защита на лични данни са разпространени до всички лица, участващи в обработката на личната информация.

4.11. Преди да получат достъп до „ВетИС“, потребителите трябва да бъдат инструктирани за работа със системата и изискванията за сигурност, за да се гарантира продуктивна и безопасна работа с данните в нея (по реда на Заповед № РД 11-2171). Запознаването на потребителите се извършва като самообучение (self-training) по предоставени от БАБХ материали, чрез обучение от друг потребител със същите или по-високи права на достъп или от администратор. Потребителите подписват „Протокол за проведено обучение“ (приложение № 5 към Заповед № РД 11-2171/25.10.2017), с изключение на самообучилите се лица.

4.12. Предоставянето на достъп до „ВетИС“ се удостоверява с „Протокол за регистриране на потребител в ИС ВетИС“ (приложение №6 към Заповед № РД 11-2171), издаден от съответния администратор (служител от дирекция ИСИС към ЦУ на БАБХ или регионален администратор от ОДБХ).

4.13. Протоколите, приложение №6, се предават на потребителите лично или чрез куриер. В тях се предоставя информация за линк за достъп до системата, потребителския профил и първоначалната парола за достъп на потребителя, съгласно „Вътрешни правила за МИС“.

4.14. Промяната и прекратяване на права за достъп до „ВетИС“ се извършва по същия ред, определен в настоящата т.4.

5. Изисквания към потребителските пароли за ИИС „ВетИС“.

При създаване и управляване на потребителски пароли в ИИС „ВетИС“ се спазват следните изисквания:

5.1. При получаването на протоколите потребителят е задължен да смени паролата си при първи достъп до системата.

5.2. При създаване и управляване на потребителски пароли в ИИС „ВетИС“ се спазват следните изисквания:

- имат най-малко 8 символа дължина;
- съдържат символи от всички от следните категории (малки букви, големи букви, цифри и специални знаци);
- не съвпадат с името на потребителя или неговия профил;
- не трябва да са базирани на лична информация, имена на членове от семейството и т.н.;
- сменят се на всеки 180 дни.

5.3. Най-малко 2 поредни пароли не могат да бъдат като предни използвани – ‘password history’. Това означава, че третата парола може да бъде като първата използвана.

5.4. При 3 неуспешни опита за въвеждане на парола потребителският профил се блокира за 15 минути. Потребителят трябва или да изчака да мине този период или да се обади на администратор от дирекция ИСИС/регионален администратор от ОДБХ да го отключи, за да може да работи.

5.5. Потребителите не трябва да използват една и съща парола за акаунти за работа с ИИС „ВетИС“ и за друг достъп извън тази система (например акаунти за лични поща, за електронна търговия и др.).

5.6. Паролите са персонални и не трябва да се предоставят на други лица по никакъв повод. Ако имат подозрение, че паролата им е станала достояние на друго лице, потребителят задължително трябва да я промени незабавно. Потребителите отговарят за всички действия, свързани с техните пароли

5.7. На потребителите се забранява да предприемат действия за научаване на личната парола на други потребители и дори да разполагат с такива пароли, да не ги използват при никакви обстоятелства.

5.8. Забранява се паролите да бъдат записвани и съхранявани във вид, който позволява свободното им прочитане. Забранява се записването на паролите в свободен текст във файлове или други места, където могат да станат достояние на неоторизирани потребители.

5.9. Забранено е изпращане на потребителски пароли по електронна поща. Изключения се допускат само за извънредни ситуации, по решение на директор дирекция ИСИС, като се изпраща временна (служебна) парола с SMS на телефона на потребителя. Потребителят е задължен да смени временната парола със своя лична при първо влизане в системата.

5.10. Не трябва да се използват функции на приложения от рода на „Запази паролата" (например в Internet Explorer, Firefox и други).

6.Управление на инциденти, свързани със сигурността на данните във „ВетИС"

6.1. Всички потребители са задължени да следят и докладват за всички забелязани или подозирани слабости в работата на **„**ВетИС". При настъпване на инциденти или събития, свързани със сигурността, потребителите уведомяват незабавно регионалния администратор в ОДБХ. При невъзможност за решаване на проблема, регионалният администратор сигнализира дирекция ИСИС към ЦУ на БАБХ чрез системата „Mantis BugTracing".

Тези потребители, които нямат достъп до „Mantis BugTracing", попълват **Приложение № 1** към настоящия наръчник /Доклад за инцидент или събитие по сигурността/.

Регионалните администратори поддържат записи за всички докладвани към тях инциденти и събития в РД ПИС 13/02-Регистър на инциденти.

6.2. При подаването на съобщение по мейл или чрез доклад за инцидент през MantisBugTraicing задължително се включва информация за вида на събитието/инцидента, например:

- неоторизиран физически достъп до устройство, чрез което се въвеждат и обработват данни в системата;
- кражба на устройство, на което има настройки за улеснен достъп до системата;
- отпадане на услуга;
- хардуерна повреда, не позволяваща достъп до системата;
- отпадане или претоварване на комуникационен канал;
- зловреден код
- нерегламентиран достъп или изтичане на информация;
- компрометиране на потребителска парола за достъп;
- нарушение на изискванията за сигурност при достъп до системата;
- загуба или повреждане на информация;
- неизправност в софтуера или друго.

6.3. Задължително се посочват уведомените лица за случая и времето на уведомяване.

6.4. Служителите от Дирекция ИСИС/регионален администратор от ОДБХ категоризират инцидента, извършват проверката на неговата достоверност, приоритизират го, предприемат действия за разрешаването му и уведомяват за това на подателя.

7. Обмен на информация чрез електронна поща

7.1. Прилагат се изискванията на приложение № 4 към „Вътрешни ИКТ правила“ – „Правила за определяне на индивидуален електронен адрес и използване на електронна поща в БАБХ“.

7.1.1. Електронната поща е собственост на БАБХ и се използва за служебни цели. Използването на електронната поща за други цели не е позволено.

7.1.2. Електронната поща се ползва лично. Потребителят не може да оторизира друго лице да чете неговата електронна поща или да изпраща съобщения от негово име. При служебна необходимост за изключения от горното правило мога да се направят с разпореждане на директора на дирекцията или главния секретар на Агенцията. Направеното изключение се документира от съответната административна единица. Документът с одобрението на ръководството се съхранява в дирекция ИСИС.

7.1.3. Паролата за ползване на електронна поща е лична и никой служител не може да я съобщава на друг, включително на системни администратори или свои ръководители.

7.1.4. Отдалеченият достъп до електронната поща се осъществява по криптиран канал (HTTPS или Exchange Active Sync).

7.1.5. Всяко съобщение, изпратено чрез електронна поща, трябва да съдържа информация за подателя с цел да се намали рискът от объркване и изтичане на информация. Тази информация включва задължително:

- име;
- телефон;
- адрес на електронна поща;
- длъжност;
- дирекция/отдел;

В края на всяко изходящо електронно съобщение автоматично се прикачва изявление за ограничаване на отговорността (disclaimer) и указания към адресата за действия при погрешно получаване.

7.1.6. Размерът на изходящите съобщения се ограничава до 25MB. По-големи съобщения се отхвърлят автоматично от сървъра за електронна поща.

7.1.7. Пощенските кутии се съхраняват на сървър в организацията до изчерпване на зададения лимит. Копие от цялата служебна поща на служителя на сървъра се пази за срок от минимум две години след напускане на служителя. По искане на прекия ръководител на служител, чийто акаунт е бил деактивиран или на директора на съответната дирекция, входящата поща за него може да се препраща автоматично към друг служител на съответния служебен адрес.

7.1.8. Съдържанието на пощенската кутия на служителя може да бъде проверявано без уведомяване на ползвателя при поискване от прекия ръководител, като се подава писмена заявка до дирекция ИСИС.

7.1.9. Всички съобщения създадени, изпратени или получени през Интернет, са собственост на БАБХ. БАБХ запазва правото си за достъп до съдържанието на всяко съобщение, изпратено чрез оборудването й, ако сметне, че дейността й има нужда да постъпи така и е правно обосновано.

7.1.10. Дирекция ИСИС има право да ограничава електронната поща според съдържанието й с оглед предотвратяване разпространението на вируси и нежелани съобщения (SPAM). Подобно ограничение се съгласува и одобрява от ръководството на БАБХ. Служителите следва да бъдат своевременно информирани за влизането в сила на всяко ново ограничение.

7.2. Ограничения при обмен на информация чрез електронна поща

7.2.1. Информация категоризирана за „Ограничено ползване“ и лични данни може да се изпраща по електронна поща, само ако е криптирана или защитена с парола.

7.2.2. При работа с електронна поща на БАБХ се спазват следните забрани и ограничения:

• не се допуска използването на електронна поща се позволява на общо основание, като това се извършва през служебни и лични мобилни устройства. Устройствата, чрез които се осъществява достъп до служебна електронна поща трябва да имат осигурена защита чрез пин или парола от компютри или други средства, които не са собственост на БАБХ ;

• забранява се използването на неслужебни e-mail адреси, за служебна комуникация, с изключение на екстремни случаи, когато липсва достъп до служебния e-mail и е необходимо да се осъществи спешна комуникация;

• забранява се използването на служебен e-mail адрес за регистриране в Интернет сайтове, с изключение на сайтове на фирми и организации с много висока репутация. При необходимост от регистрация в сайт, неотговарящ на тези изисквания, трябва да се използва e-mail адрес от публични сайтове за предоставяне на e-mail услуги (например от Yahoo, GMail и други);

• забранява се автоматичното препращане на служебния e-mail към външни e-mail адреси ;

• забранява се отварянето на прикрепени файлове от входящи съобщения, преди да са се убедили, че антивирусният софтуер работи;

• забранява се отварянето на прикрепени файлове от входящи съобщения от неизвестни и съмнителни изпращачи. Във всички случаи при получаване на съмнителни файлове прикачени към електронната поща, дори и подателя да изглежда познат, те не бива да се отварят ако няма потвърждение за съдържанието им по друг начин (например телефонен разговор с подателя). В такива случаи незабавно се уведомява служител на дирекция ИСИС. Съответния служител на дирекция ИСИС може да поиска подозрителното съобщение да му бъде препратено и / или изтрито;

• забранява се изпращането на нежелани писма (спам);

• забранява се изпращането на материали, съдържащи вируси, програмен код, предназначен за осъществяване на несанкциониран достъп, възпрепятстване или ограничаване на функционалността на компютърно или комуникационно оборудване или друг нежелан от получателя код;

• забранява се изпращането на имена, пароли и други средства за получаване на несанкциониран достъп до платени ресурси в Интернет, както и препратки към такава информация;

• забранява се разпространяването на материали, защитени от авторски права, търговска марка, търговска тайна и други, включително серийни номера за програмни продукти и програми за генериране на такива номера;

• забранява се разпространяването на информация, съдържанието на която е забранено от международното или българското законодателство, включително материали със заплашително, оскърбително, клеветническо, дискриминационно и непристойно съдържание;

• забранява се разпространяването на материали, подстрекаващи към насилие, междуособни конфликти и противозаконни прояви, в това число разясняващи начина на използване на взривни вещества и оръжие;

• забранява се разпространяването на чувствителна информация, станала им известна в процеса на работа или по някакъв друг начин, както и информация, която

може да бъде третирана по смисъла на Закона за защита на класифицираната информация и Закона за защита на личните данни, с изключение, когато разпространението се извършва на база законови или договорни изисквания

8. Правила за използване на Интернет

8.1. Всички, които ползват мрежата на БАБХ, имат право на достъп до интернет единствено и само за изпълнение на служебните си задължения и конкретно поставени задачи.

8.2. Въвеждат се следните ограничения и забрани:

- за всички, които ползват мрежата на БАБХ, е забранен достъпа (съответно действия с файлове) до сайтове с развлекателен характер и нецензурно и/или със съдържание, противоречащо на законодателството на Р.България и Европейската общност. Това се отнася и до действия, чийто резултат представлява нарушение на споменатите законодателства;
- забранени са действия, които могат да доведат до проблеми със сигурността или работоспособността на външни мрежи, като например: действия свързани със сканиране на портове на сървъри и/или мрежи, изпращане на множество заявки към сървър, с цел претоварването му, опити за преодоляване на защитни механизми на сървъри и/или мрежи и др.;
- не се допуска използване на Интернет ресурси за лични нужди и облаги. Категорично се забранява изтеглянето от интернет на файлове съдържащи филми, музика и други развлекателни материали;
- екипът за системно администриране, след съгласуване с директорът на дирекция ИСИС, има право да налага ограничения за достъп и до други сайтове, изтегляне (download) на файлове и други услуги, които могат да доведат до проблеми със сигурността или работоспособността на мрежата на БАБХ и/или електронните услуги, предоставяни от него.
- забранено е изтеглянето от Интернет на изпълними файлове (програми, скриптове и други подобни), включително и такива във архивен формат (ZIP, RAR и др. подобни). При необходимост от използване на софтуер, който се достъпва или получава чрез Интернет, той се заявява на дирекция ИСИС.
- дирекция ИСИС използва технически средства за ограничаване възможността за изтегляне от Интернет на неразрешени файлове и посещаване на неразрешени сайтове;
- максималната скорост, с която може да се получава информация от Интернет от едно потребителско работно място подлежи на ограничаване съобразно нуждите и възможностите на наличните канали за връзка с Интернет. При технически проблем или друга техническа причина е възможно скоростта на достъп на потребителите да бъде ограничена допълнително, за да се осигури нужния капацитет за нормална работа на критични за дейността на БАБХ приложения свързани с използване на Интернет ресурса;
- в случаите, когато за изпълнение на служебни ангажименти се изискват действия в противоречие на настоящата политика и „Вътрешните ИКТ правила“, същите се извършват след писмено разрешение на главния секретар на БАБХ, съгласувано с директорът на дирекция ИСИС. Дирекцията-заявител описва: причината, вида и времевия период за подобно действие, имената на служителя и компютъра от който ще се извърши. Копие на документа с разрешението на главния секретар на БАБХ се предава за изпълнение на дирекция ИСИС, което се съхранява най-малко 12 месеца.

9. Информационна сигурност, свързана с персонала на БАБХ

9.1. Като част от договорните им задължения, служителите В БАБХ подписват декларации при постъпване на работа, в които се посочват задълженията им за опазване сигурността на информацията, като между тях са:

а) Декларация по §1 от Постановление № 57 на Министерски съвет от 2 април 2020 г. за приемане на Кодекс за поведение на служителите в държавната администрация;

б) Декларация по чл.45, ал.2 от Етичния кодекс за поведение на служителите в Българската агенция по безопасност на храните.

9.2. Служителите на БАБХ, на които е предоставен достъп до информация и средства за обработка на информация в БАБХ , между които и „ВетИС“, се запознават с:

а)отговорностите и правата им според действащото законодателство, вътрешните регламенти („Вътрешни правила МИС“ и „Вътрешни правила ИКТ“) и настоящия Наръчник;

б) отговорностите при ползването на информационните системи и активи на БАБХ, с които боравят, между които и „ВетИС“;

в) дисциплинарни действията и санкции, които ще се предприемат, ако служителят пренебрегва изискванията за сигурност.

9.3. По преценка на ръководството на БАБХ, отговорностите, свързани с опазване на информационната сигурност, могат да продължат за определен период след прекратяване на договора.

9.4. Обучение по информационна сигурност

9.4.1. Обучения на потребителите на ИИС „ВетИС“ от ЦУ на БАБХ и ОДБХ за работа със системата се провеждат съгласно вътрешна Заповед №РД-11/2171/25.10.2017 г. на ИД и последващи изменения.

9.4.2. Обучението се провежда преди получаване на достъп до ИИС „ВетИС“ и е съобразено с определените задължения на потребителите.

9.4.3. Обучението на потребителите се извършва от разработчика на системата или от друг потребител, който има права за потребителската група, за която се отнася обучението. За проведеното обучение на потребители на „ВетИС“ се изготвя протокол – Приложение №5 към Заповед №РД-11/2171/25.10.2017 г.

9.4.4. В допълнение, всички потребители на ВетИС, които са служители на БАБХ, получават по утвърден от ръководството План-график подходящо обучение по опазване на информационната сигурност, съответстващо на заеманата от тях длъжност/роля. Това обучение включва запознаване с приложимите за потребителя политики и правила по ИС, включително и с настоящия „Наръчник на потребителя на ВетИС“ и се документира с „Протокол от проведено обучение“ (свободна форма), който се съхранява в дирекция ИСИС.

9.5. Дисциплинарни мерки

Конкретни дисциплинарни мерки са определени и се прилагат в съответствие с глава VII „Дисциплинарна отговорност“ на „Вътрешни правила ИКТ“. В БАБХ има постоянно действащ дисциплинарен съвет, на който се разглеждат и се вземат решения относно конкретни дисциплинарни мерки спрямо служители, нарушили вътрешните правила, свързани с информационната сигурност.

9.6. Отговорности при смяна на длъжността или напускане

Отговорностите при смяна на длъжността са съобразени с характера на новите отговорности на служителя. Ако тези задължения включват работа с „ВетИС“,

задължително се прилагат изискванията, залегнали в т. 9.4.1, преди предоставяне на достъп до системата.

9.7. При прекратяване на достъпа на потребител

9.7.1. При прекратяване на достъпа на потребител до информационните системи на БАБХ, включително и до „ВетИС“, се прилагат изискванията на глава V „Прекратяване на служебното или трудовото правоотношение на служителите в БАБХ“ от „Вътрешни правила ИКТ“.

9.7.2. При необходимост, при напускане служителят поема определени задължения, свързани с изискванията за информационна сигурност. Отговорностите и задълженията, които ще важат след напускане, се съдържат в договорите на служителите/актовете за назначаването им.

9.8. Връщане на активи

9.8.1. Всички служители, при напускане или прекратяване на договора връщат на БАБХ всички активи, които са им били предоставени. Освен връщането на материалните активи - придобити програми, документи и оборудване (преносими компютри, флаш памети, преносими дискове, карти за достъп, софтуер, ръководства и информация, съхранявана на електронни носители и други. Прилагат се изискванията на глава V „Прекратяване на служебното или трудовото правоотношение на служителите в БАБХ“ от „Вътрешни правила ИКТ“.

9.8.2. С получаване на заповедта за освобождаване от длъжност служителят предава на прекия си ръководител служебно ползваните информации, акаунти и пароли, включително и за достъп до „ВетИС“, спазвайки процедурите, описани в Приложение № 10 към „Вътрешни правила ИКТ“. За връщането на активи се подписва „Приемо-предавателен протокол“.

9.8.3. В случаите, когато служител е използвал свое лично оборудване, се спазват процедури гарантиращи, че цялата съответна информация е прехвърлена обратно към организацията и е сигурно изтрита от оборудването.

9.8.4. В случай, че напускащият или сменил позицията си служител, притежава информация, включително и да работата във „ВетИС“, която е важна за продължаване на работата, тя се документира и предава на организацията. Отговорност за това носи прекия ръководител.

9.8.5. При преместване на нова длъжност, която не изисква достъп до „ВетИС“, се премахват правата за достъп до системата. Анулират се или се променят всички действащи пароли за достъп.

10. Работа с обозначена и категоризирана информацията

10.1. В БАБХ е въведена система за обозначаване на обработваната информация. Документи, генерирани от „ВетИС“ и такива, които се създават на база информацията от „ВетИС“, не подлежат на маркиране. Общодостъпната информация не се маркира.

10.2. Ако по погрешка информация, обозначена „За служебно (вътрешно) ползване“ или „Ограничено ползване“ попадне при външен потребител на „ВетИС“, той е длъжен да не я обработва или разпространява и да информира подателя, по начин, гарантиращ защита от неправомерно разкриване пред трети страни.

№ по ред		Версия	Редакция	Описание на промените

ДОКЛАД ЗА ИНЦИДЕНТ ИЛИ СЪБИТИЕ ПО СИГУРНОСТТА

Име	**Фамилия**
Длъжност	**Телефон**
Структурно звено	**Дата, час**

ПОДРОБНОСТИ ЗА ИНЦИДЕНТА/СЪБИТИЕТО (*попълва се от лицето, което докладва*) **Описание на инцидента/събитието:** **Подпис на лицето, докладвал инцидента:……**	
Приел доклада:…….. **(*име, фамилия, дата, час, подпис*)**	
Категория на инцидента (*Информацията се попълва се от служителя приел/обработил доклада*)	
☐ Неоторизиран физически достъп до устройство, чрез което се въвеждат и обработват данни в системата.	☐ Отпадане на услуга
☐ Кражба на устройство, чрез което се въвеждат и обработват данни в системата;	☐ Отпадане или претоварване на комуникационен канал
☐ Хардуерна повреда, непозволяваща достъп до системата	☐ Изтичане на информация
☐ Зловреден код	☐ Загуба или повреждане на информация
☐ Нарушение на политика за сигурност	☐ Неизправност в софтуера
☐ Неизправност в софтуера	☐ Нарушение на изискванията за сигурност при достъп до системата
☐ Компрометиране на потребителска парола за достъп.	☐ Друго……..
Уведомени лица (*Информацията се попълва се от служителя приел/обработил доклада*): ☐ Председател на групата по управление на СУСИ ☐ Отговорник по информационна сигурност към СУСИ ☐ Член на групата по управление на СУСИ: …….. ☐ Друг служител на дирекция ИСИС…… ☐ Системен администратор в …….. ☐ Регионален администратор в ОДБХ ……	
Ниво на инцидента (1-4):…….. **(*Информацията се попълва се от служителя приел/обработил доклада*)** **Дата/Час:……** **Подпис: ……..**	
Предприети действия:	