# ДЕКЛАРАЦИЯ

## ОТ РЪКОВОДСТВОТО НА „ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД

**ВИСШЕТО РЪКОВОДСТВО** на **„ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД (СЪВЕТА на ДИРЕКТОРИТЕ чрез Оперативното ръководство на дружеството)** приема **ПОЛИТИКА** за поддържане и непрекъснато подобрение на система за управление на сигурността на информацията, съответстваща на международния стандарт **ISO/IEC 27001:2013**, като средство за утвърждаване доброто име и репутация на дружеството и за създаване на възможности за превантивност и непрекъснато подобряване.

**Управлението на сигурността на информацията** в **„ТОПЛОФИКАЦИЯ СОФИЯ" *ЕАД*** в определения физически обхват е дефинирано, като защита на наличната и използваната информация свързана с личните данни на своите клиенти, доставчици и собствен персонал, както и информацията свързана с техническото осигуряване на всички работни процеси от широк кръг идентифицирани заплахи, за да се гарантира непрекъсваемостта на работните процеси в дружеството и да се минимизират загубите при евентуални аварии, инциденти, природни бедствия и др.

Дефинирането, постигането, поддържането и подобряването на управлението на сигурността на информацията в **„ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД** е от съществено значение за запазване и подобряване нивото на удовлетвореност на единичните ни клиенти и бизнеса, както и за осигуряване на законосъобразност и изпълнение на договорните задължения.

Ръководство на ***„ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД*** декларира следната своя ***ОФИЦИАЛНА ПОЛИТИКА ПО УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА***:

***„Системата за управление на сигурността на информацията (СУСИ) на „ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД включва рамка, в която ясно са дефинирани целите и принципите на сигурността на информацията, като едновременно с това създава ясни критерии за оценка на рисковете към наличните информационни активи.***

***СУСИ е съобразена с всички административни, договорни, правни и нормативни изисквания на процесите по постигане на необходимото ниво на доверие, задължения за осигуряване на ниво на сигурност и отговаря на стратегическия контекст за управление на риска към информационните активи в „ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД.***

***Ръководството декларира, че главната цел е да създава доверие, като предоставя на своите клиенти, партньори и заинтересовани страни доставяне на своя продукт и съпътстващите го услуги, които съответстват на техните изисквания за сигурност, като едновременно с това гарантира поверителост, цялостност и достъпност до наличните информационни активи, осигуряващи процесите на:***

***ПРОИЗВОДСТВО И ПРЕНОС НА ТОПЛИННА ЕНЕРГИЯ.***
***ПРОИЗВОДСТВО НА ЕЛЕКТРИЧЕСКА ЕНЕРГИЯ. ДЯЛОВО РАЗПРЕДЕЛЕНИЕ. ПРОЕКТИРАНЕ, ИЗГРАЖДАНЕ, РЕМОНТ И ПОДДРЪЖКА НА ТОПЛОИЗТОЧНИЦИ, ТОПЛОПРЕНОСНИ МРЕЖИ И АБОНАТНИ СТАНЦИИ в две основни направления:***

- ***Управление на информационни активи свързани с клиенти, доставчици и персонала на дружеството;***
- ***Непрекъснатост на работата и кризисно управление.***

***Ръководството ще се стреми да осигури и поддържа максимално ниво на сигурност (покриване с внедрени ефикасни механизми на контрол на не по-малко от 95% на наличните информационни активи), касаещи предоставянето на регламентираните дейности, като не приема под никаква форма използването на нелицензиран или „пиратски" софтуер и приложения.***

***Ръководството на дружеството дълбоко е убедено, че това може да бъде постигнато с осигуряване и поддържане на мотивираност, компетентност на персонала и съпричастност към извършваната работа от всеки служител, с цел постигане на устойчивост на добрите резултати.***

***Изпълнени са редица мероприятия, с които са оценени съществуващите заплахи и е определен риска към съответните информационни активи, като е взето решение да бъдат планирани и предприети мероприятия за въздействие и управление на рискове към информационни активи оценени със статут „ВИСОК" и „ИЗИСКВАЩ ВНИМАНИЕ" съгласно приета СТРАТЕГИЯ ЗА ОЦЕНКА НА РИСКА.***

За целите на управление на сигурността на информацията, в допълнение към основната политика и нормативно заложените към нас изисквания са дефинирани, документирани и внедрени ***регламенти и* НАБОР *политики за*:**

- *РЕЗЕРВИРАНЕ НА ИНФОРМАЦИЯ*
- *ПРИЕМЛИВО ИЗПОЛЗВАНЕ НА ИНФОРМАЦИОННАТА СИСТЕМА*
- *КОНТРОЛ НА ДОСТЪПА. ЧИСТО БЮРО И ЗАЩИТЕН ЕКРАН*
- *УПРАВЛЕНИЕ НА ПАРОЛИ*
- *ВЗАИМООТНОШЕНИЯ С ВЪНШНИ СТРАНИ И ДОСТАВЧИЦИ*
- *ИЗПОЛЗВАНЕ НА МРЕЖОВИ УСЛУГИ И НОСИТЕЛИ*
- *МОБИЛНИ СРЕДСТВА И РАБОТА ОТ РАЗСТОЯНИЕ*
- *КОМУНИКАЦИИ С ЕЛЕКТРОННА ПОЩА*
- *КРИПТОГРАФСКИ МЕХАНИЗМИ ЗА КОНТРОЛ*

***Политиките по сигурност на информацията и всички документирани процедури и регламенти са задължителни за изпълнение от целия персонал, работещ в и за „ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД, тъй като напълно оценяваме значителността на дружеството и последствията, които могат да настъпят при компрометиране на сигурността на обекти от критичната инфраструктура на страната.***

***В качеството си на ИЗПЪЛНИТЕЛЕН ДИРЕКТОР на „ТОПЛОФИКАЦИЯ СОФИЯ" ЕАД поемам ангажимента и лична отговорност да осигурявам всички необходими ресурси за изпълнение на изискванията за сигурност на информацията. С настоящата декларация Ръководството на „Топлофикация София" ЕАД приема ангажиментите, поети съгласно декларацията от 10.06.2015г.***

***СОФИЯ, 30.03.2018 г.***
***ИЗПЪЛНИТЕЛЕН ДИРЕКТОР***
***Сашо ЧАКАЛСКИ***

топлофикация
софия ЕАД

# НАБОР ПОЛИТИКИ ПО СИГУРНОСТ

ИНТЕГРИРАНА СИСТЕМА ЗА УПРАВЛЕНИЕ

## [ПС]

| Разработил: | Съгласувал: | Утвърдил: |
|---|---|---|
| Веселин ДИМИТРОВ | Мариана ПОПОВА | Георги БЕЛОВСКИ |
| Подпис: | Подпис: | Подпис: |

**ЕКЗЕМПЛЯР:**

☒ Контролиран ❑ Оригинал

❑ Неконтролиран ❑ Копие ☒ Електронно копие

**Предназначение:** Настоящият набор от политики дефинира управлението на дейности и процеси свързани със системата за управление на сигурността на информацията. Целта на тези политики е да въведе единен подход при изпълнението на регламентираните изисквания.

**Обхват:** Действието на тази политики обхваща длъжностните лица, които използват или отговарят за информационни активи на „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД.

За прилагането и спазването на тези политики носят отговорност РЪКОВОДСТВО (ИД, ЗАМ. ИД, ПР, ЕРГСИ (Експертна работна група по сигурност на информацията), ИКТ и всички длъжностни лица от дружеството, на които са възложени задачи свързани със сигурност на информацията – пряко или косвено.

**Забележка:** *Всички документи и данни са под формата на всякакъв носител, като хартиено копие, снимков материал, електронен носител и др.*

**ДИСЦИПЛИНАРЕН КОНТРОЛ:** ЗАДЪЛЖЕНИЕ НА ВСЕКИ КОМПЮТЪРЕН ПОТРЕБИТЕЛ Е ДА ЗНАЕ ТЕЗИ ОСНОВНИ ПРИНЦИПИ И ДА ГИ ПРИЛАГА ПРИ СВОЯТА ДЕЙНОСТ.

ВСЯКО ДЛЪЖНОСТНО ЛИЦЕ НАРУШИЛО ТЕЗИ ПОЛИТИКИ МОЖЕ ДА Е ОБЕКТ НА ДИСЦИПЛИНАРНО НАКАЗАНИЕ, ВКЛЮЧИТЕЛНО И ДИСЦИПЛИНАРНО УВОЛНЕНИЕ.

==========

СЪДЪРЖАНИЕ:



==========

## (ПС-01)

## РЕЗЕРВИРАНЕ НА ИНФОРМАЦИЯ

Надеждното съхранение на информацията е важен аспект от компютърната сигурност. Редовното резервиране на информацията е от голямо значение при непредвиден срив в системата при който може да се загуби част или цялата информация в сървърите на дружеството. Своевременното архивиране може да помогне за бързо възстановяване на работоспособността на информационната система без сериозни загуби на информация.

Автоматизирано и планово се извършва резервиране на цялата работна информация на сървърите което включва:

- Инсталирани програмни продукти и приложения;
- Бази данни на всички програмни продукти;
- Различни видове документи;

Резервирането на данните се извършва така, че да могат при необходимост да бъдат инсталирани на друг сървър и да се продължи работния процес без чувствителна загуба на данни.

1. Всички бази данни, файлове и програмни продукти инсталирани на съответните сървъри се архивират в извънработно време.
2. За архивирането отговаря системния администратор.
3. Подробна информация относно времето и последователността на резервирането на информация е указан в
   „ГРАФИК РЕЗЕРВИРАНЕ“

ГРАФИК РЕЗЕРВИРАНЕ.xlsx (Права на достъп: Системен администратор)

4. Резервни архиви на SMDC се извършват на всеки 168 часа съгласно настройките от контролния панел на приложението.
5. Архиви от видеонаблюденията се съхраняват до 30 (тридесет) дни.

==========

**(ПС-02)**

## ПРИЕМЛИВО ИЗПОЛЗВАНЕ НА ИНФОРМАЦИОННАТА СИСТЕМА

### Използване и права на собственост

1. Потребителите знаят, че данните, които създават използвайки информационните системите и устройства са собственост на „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД или на нейните клиенти или заинтересовани страни.
2. Всяка информация, която потребителите определят като чувствителна или уязвима е управлявана.
3. Ръководството на дружеството си запазва правото да проверява компютърното оборудване периодично за да гарантира съответствие с тази политика.

### Сигурност на информацията

1. Служителите трябва да предприемат всички необходими стъпки за да предотвратят неоторизиран достъп до поверителна/конфиденциална за дружеството информация (фирмена тайна). Примери за поверителна информация са, но не се ограничава само до: поверителна за дружеството вътрешна информация, поверителна информация съгласно нормативни актове или договорни изисквания, лични данни и др.
2. Дръжте паролите защитени и не споделяйте акаунти. Служителите са отговорни за защитата на техните пароли и акаунти. Паролите за достъп на системно ниво трябва да бъдат променяни на всеки 3 (три) месеца, а потребителските пароли на всеки 6 (шест) месеца.
3. Не се позволява неоторизиран запис и пренос на информация в преносими носители (CD, flash памети и др.) тъй като тя може да е уязвима, освен в случай на предаване на болнични листове или аналогична по статус информация към НОИ/НАП и др. чрез дискети – за целта след извършване на преноса, информацията следва да бъде изтрита от устройството.
4. Всички носители подлежащи на бракуване (след повреда или негодност) се унищожават чрез трайно нарушаване на физическата цялост – дискове, дискети и др. – чрез счупване на две части).
5. Регистрирането на служители в нюзгрупи с E-mail адреса на дружеството трябва да съдържа изрично уточнение, че мнението изложено от служителя е лично негово, а не на дружеството, освен в случаите, когато това е свързано с дейността на фирмата.
6. Всички компютри на дружеството редовно се сканират за вируси със софтуер с актуални вирусни сигнатури.
7. Служителите трябва да бъдат изключително внимателни при отварянето на прикачени файлове към E-mail получен от неизвестен източник, тъй като те може да съдържат вируси, кодове на “троянски коне” и т. н.

**Неприемливо използване. Следните дейности са напълно забранени!!!**

При никакви обстоятелства служител на дружеството извършващ дейности, които са противозаконни по силата на законодателството на Република България или международни закони не трябва да използва ресурси собственост на дружеството. Изброеното по долу не е изчерпателен списък, но се стреми да обхване групата от действия, които попадат в категорията за не приемливо използване.

ЗАБЕЛЕЖКА:

*Определени служители може да не спазват тези ограничения по време на изпълнението на служебните си задължения (например: системните администратори може да имат нужда да забранят мрежовия достъп до определен хост, ако този хост пречи на нормалната работа на предоставяните услуги и др.).*

**СЛЕДНИТЕ ДЕЙСТВИЯ СА СТРОГО ЗАБРАНЕНИ БЕЗ НИКАКВИ ИЗКЛЮЧЕНИЯ!!!:**

1. Нарушаване на права защитени по силата на закон (лични данни, авторски права на използван софтуер и т. н.), търговска тайна, патенти или други подобни, ***инсталирането или разпространението на "пиратски" или друг вид нелицензирани софтуерни продукти***, за които дружеството не притежава съответни лицензи. Копирането без съответното упълномощаване от собственика на материали защитени с авторски права включващи, но не ограничени до сканиране и разпространение на фотографии от списания, книги и други източници обект на авторки права, защитена с авторски права музика, а също така и инсталиране на лицензиран софтуер, за който дружеството или крайните потребители нямат съответните лицензи е строго забранено!.
2. Изнасянето от дружеството на хардуер, софтуер и технологии без разрешение от страна на Управителя или Изпълнителния директор е СТРОГО ЗАБРАНЕНО.
3. Вкарването на злонамерени програми в компютърното оборудване (например: вируси, „червеи", „троянски коне", E-mail бомби и др. подобни).
4. Разкриването на личната парола или позволяването на използването на вашия акаунт от други личности. Това включва и членовете на семейството, когато се работи при необходимост отдалечено от къщи.
5. Използването на компютърните активи на дружеството за разпространение на порнографски и други забранени от закона материали.
6. Изготвяне на лъжливи данни за услуги от името на дружеството.
7. Приемане на задължения явно или косвено, ако те не са част от нормалния процес на работа.
8. Последици от нарушаване на сигурността или разрушаване на мрежовата комуникация. Нарушенията в сигурността включват, но не се ограничават до достъп до данни, за които служителя не е упълномощен да има достъп, получаване на достъп или включване към сървър или акаунт, за който служителя не е изрично упълномощен да има достъп освен, ако това не е част от обичайните му служебни задължения.
9. Сканирането на портове или сканирането за уязвимости в мрежовата сигурност е строго забранено, ако преди това не е уведомен системен администратор.
10. Осъществяването на всякакъв вид мониторинг на компютърното оборудване, който прихваща потребителските данни, освен ако тази дейност не е част от нормалните задължения на служителя.
11. Заобикалянето на автентикацията на потребителя или политиките за сигурност, на който и да е хост, мрежа или акаунт.
12. Блокирането или отказа на услуга на потребител различен от хоста на служителя;
13. Предоставянето на информация или списъци със служителите на дружеството на други лица.

==========

**(ПС-03)**

**КОНТРОЛ НА ДОСТЪПА. ЧИСТО БЮРО И ЗАЩИТЕН ЕКРАН**

В ДРУЖЕСТВОТО Е ПРИЕТА **ПОЛИТИКА ЗА *„ЗАЩИТЕН ЕКРАН"*** - ВСИЧКИ СТАЦИОНАРНИ КОМПЮТРИ СА ЗАЩИТЕНИ С PASSWORD-PROTECTED SCREENSAVER, КОЙТО СЕ АКТИВИРА НАЙ-МАЛКО СЛЕД 10 (ДЕСЕТ) МИН. ИЛИ ПОСРЕДСТВОМ LOGGING-OFF (CONTROL-ALT-DELETE ЗА WIN2K И XP ПОТРЕБИТЕЛИТЕ), КОГАТО ХОСТА НЕ СЕ ИЗПОЛЗВА.

В ДРУЖЕСТВОТО Е ПРИЕТА **ПОЛИТИКА ЗА *„ЧИСТО БЮРО*** – ВСЯКАКЪВ ВИД ИНФОРМАЦИЯ, КОЯТО Е КАТЕГОРИЗИРАНА КАТО „ФИРМЕНА ТАЙНА“, НЕЗАВИСИМО ОТ ЕСТЕСТВОТО НА НЕЙНИЯ НОСИТЕЛ, НЕ МОЖЕ ДА БЪДЕ ОСТАВЯНА НА ПУБЛИЧНИ МЕСТА ИЛИ МЕСТА (бюра, маси, шкафове и др.) С ВЪЗМОЖЕН ДОСТЪП ОТ НЕОТОРИЗИРАНИ ЛИЦА.

a) Да се установи рамка за управление, която да контролира, внедряването и усъвършенстването на информационната сигурност в дружеството.
b) Определяне инфраструктурата на сигурността и дефиниране на правомощията по сигурността на отделните длъжностни лица и служителите от различните направления на дейност.
c) Да се контролира достъпът до информация.
d) Да се предотврати нерегламентираният достъп до информационните системи.
e) Да се предотврати нерегламентираният достъп на потребители.
f) Защита на мрежовите услуги.
g) Да се предотврати нерегламентираният компютърен достъп.
h) Да се предотврати нерегламентирания достъп до информацията, съдържаща се в информационните системи.
i) Да се открие нерегламентирана намеса.
j) Да се обезпечи сигурност на информацията при използване на преносими компютри и средства за дистанционна работа.

В ДРУЖЕСТВОТО Е ПРИЕТА **ПОЛИТИКА ЗА ФИЗИЧЕСКИ КОНТРОЛ НА ДОСТЪПА –** ВСИЧКИ ПОДСТЪПИ КЪМ АДМИНИСТРАТИВНИТЕ И РАБОТНИ СГРАДИ СЕ ИЗВЪРШВАТ ПОСРЕДСТВОМ ВХОД С ИДЕНТИФИКАЦИОННИ КАРТИ, РЕГИСТРИРАНЕ И ВИДЕОНАБЛЮДЕНИЕ.

- **Оперативни изисквания за контрол на достъпа**

Достъпът до информацията и процесите е контролиран.

Той е съобразен с политиката по разпространение на информацията.

**Политика и изисквания на процесите:**

Изискванията към контрол на достъпа в дружеството са определени и документирани. Ръководството на „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД има ясно обявени правила за контрол на достъпа и права за всяка група потребители.

Политиката е съобразена с:

a) изисквания към сигурността на отделните направления, касаещи дейността;
b) определяне на цялата информация, свързана в направления, касаещи дейността;
c) политиката по разпространение на информацията и упълномощаване, т.е. необходимостта от познаване на принципите, степента на сигурност и класификацията на информацията.
d) съвместимостта между контрола върху достъпа и политиката за класифициране на информацията, за различните системи и мрежи;
e) съответстващо законодателство и всички договорни задължения по отношение на защита на достъпа до данни или услуги;
f) стандартни потребителски профили за често срещаните категории задачи;
g) управление на правата за достъп в разпределена и мрежова среда, която разпознава всички видове налични връзки.

**Правила за контрол на достъпа**

При определяне на правилата за контрол на достъпа се отчита:

a) различаването между правила, които винаги трябва да се прилагат строго и правила, които не са задължителни или зависят от определени условия;

b) установяването на регламенти, основани на правилото ***„Какво трябва да е забранено, освен ако не е изрично разрешено"***, вместо по-малко категоричното правило *"Всичко е разрешено, освен ако не е изрично забранено"*;
c) измененията в етикетите на информацията, които се извършват автоматично от средствата за обработка на информацията и такива, които се извършват по преценка на потребителя;
d) измененията в разрешенията за потребителите, които се извършват автоматично от информационната система и такива, извършвани от администратор;
e) правилата, които изискват утвърждаване от администратор или от някои друг, преди да бъдат задействани и такива, които не изискват това.

➢ **Управление на достъпа за потребителите**

В дружеството има установени процедури за достъп до информационните системи и услуги.

Процедурите обхващат всички етапи от цялостния процес на достъп на потребителите, от първоначалната регистрация на нови потребители до окончателното прекратяване на регистрацията на потребители, които не се нуждаят повече от достъп до информационните системи и услуги.

**Регистрация на потребителите**

Достъпът до информационните услуги за множество потребители се контролира чрез официален процес на регистрация на потребителя, който включва:

a) проверка на разрешението, което потребителят има от притежателя на системата за ползване на информационната система или услуга. Може също така да бъде уместно отделно утвърждаване на правата за достъп от ръководството на системата;
b) проверка на това, дали равнището на дадения достъп е подходящо за целите и дали е съвместимо с политиката по сигурността на то, например, дали не влошава разделянето на задълженията;
c) изискване от потребителите да подписват декларации, показващи че те разбират условията за достъп и поверителност/конфиденциалност;
d) осигуряване, че доставчиците на услуги не дават достъп преди да са завършили процедурите по упълномощаване;
e) поддържане на официален регистър на всички служебни лица, регистрирани за достъп до информационната система;
f) незабавно отнемане на правата за достъп на потребители, които са сменили длъжността си или са напуснали администрацията;
g) периодични проверки за наличие на повтарящи се идентификации на потребители и разрешения за ползване и отстраняването им;
h) осигуряване, че не се издават повтарящи се идентификации на други потребители.

Ръководството на дружеството включва клаузи (декларации за поверителност/конфиденциалност) в договорите за работа на персонала и договорите за външни услуги. Тези клаузи определят санкции при предприемане на нерегламентиран достъп от страна на персонала или на тези, които предоставят външните услуги.

**Управление на привилегии**

Предоставянето и ползването на привилегии са ограничени и контролирани.

Достъп до помещенията в извън работно време е ограничен и се контролира от денонощната охрана и видеонаблюдение.

**Управление на паролите на потребителите**

Паролите са общоприето средство за потвърждаване на самоличността на потребителя за достъп до информационна система или услуга.

Даването на пароли става контролирано чрез формализиран процес на управление, който изисква:

a) да се изисква от потребителите да подпишат декларация за запазване на поверителността/конфиденциалността на личната парола и на групови пароли (ако има такива), единствено в рамките на членовете на групата (това може да бъде включено в условията и изискванията за назначаване на работа);
b) да се осигури, че когато потребителите трябва да поддържат свои собствени пароли, те трябва да бъдат давани първоначално със сигурна временна парола, която те са длъжни да сменят незабавно. Временните пароли, давани в случай, че потребителите забравят паролата си, трябва да бъдат давани само след категорично идентифициране на самоличността на потребителя;
c) да се изисква временните пароли да бъдат давани на потребителите по сигурен начин. Използването на трети страни или незащитени (с обикновен текст) съобщения по електронната поща трябва да бъдат избягвани. Потребителите трябва да потвърждават получаването на паролите.

Паролите не се съхраняват в компютърната система в незащитен вид.

Администраторските пароли за достъп и управление на информационни системи се съхраняват на хартиен и магнитен носител в ИКТ в метална каса с контролиран достъп.

Достъп до тях има системните администратори при необходимост.

**Преглед на правата за достъп на потребителите**

За да се поддържа ефективен контрол върху достъпа до данни и информационни услуги, в общинска администрация се провежда регулярно официален процес за преглед на правата за достъп на потребители, така че:

a) правата за достъп на потребителите да се преглеждат през регулярни интервали от 6 (шест) месеца, освен ако няма изменения, свързани с промяна в статуса на персонала (напускане, назначаване, преназначаване, уволнение, смърт / в срок до 24 часа се прекратяват правата на достъп) – информацията се получава от Дирекция „ЧОВЕШКИ РЕСУРСИ“
b) упълномощаването за специални привилегировани права за достъп се преглежда на интервали от 3 (три) месеца;
c) дадените привилегии се проверяват на регулярно за да се осигури, че не са били давани неразрешени привилегии.

**Отговорности на потребителите**

Ръководството на дружеството прави всичко възможно потребителите да осъзнават своята отговорност за поддържане на ефикасни мерки за контрол на достъпа.

**Използване на пароли за достъп**

Потребителите следват препоръчителните практики за сигурност при избора и използването на пароли.

Паролите са средство за потвърждаване на самоличността на потребителя и по този начин да се установят права за достъп до средствата или услугите за обработка на информацията.

Всички потребители се инструктират:

a) да пазят конфиденциалността на паролите;
b) да избягват записването на пароли върху лист хартия, освен ако те могат да бъдат сигурно съхранявани;
c) да сменят паролите винаги, когато има каквито и да са индикации за това, че системата или паролата са били изложени на риск;
d) да избират качествени пароли с минимална дължина от шест символа, които са:
    - лесни за запомняне;
    - не са основани на нещо, което друг може лесно да отгатне или да получи, като използва информация, свързана с личността, например имена, телефонни номера, рождени дати и т.н.;
    - да няма последователни еднакви символи или изцяло цифрови или изцяло буквени групи.

e) да сменят паролите на редовни интервали от време или през определен брой влизания в системата (паролите за привилегированите потребителски права трябва да бъдат сменяни по-често от нормалните пароли) и да избягват повторното използване или ротацията на стари пароли;
f) да сменят временните пароли при първото регистриране в системата;
g) да не включват паролите в какъвто и да е автоматизиран процес на регистрация, например, запазени в помощна програма или извикването им с функционален клавиш;
h) да не използват индивидуалните пароли съвместно с други потребители.

При необходимост от достъп до повече услуги или платформи се използва единична, качествена парола за всички услуги, които осигуряват приемлива степен на защита на съхранените пароли.

**Оборудване с достъп до потребители, оставени без наблюдение**

В дружеството не се оставя отговорно оборудване без охрана и наблюдение.

**Контрол на достъпа до мрежи**

Достъпът, както до вътрешни, така и до външни мрежови услуги е контролиран. Така се гарантира надеждността на достъпа до мрежи и мрежови услуги, не излагат на риск сигурността на тези мрежови услуги, като обезпечават:

a) подходящи интерфейси (връзки) между мрежата на дружеството и мрежи, принадлежащи на други организации или обществени мрежи;
b) подходящи механизми за удостоверяване на самоличността за потребители и оборудване;
c) контрол на достъпа на потребителите до информационните услуги.

В дружеството не се осигурява нерегламентиран достъп на клиенти и други външни лица до мрежи и са разработени защитни механизми по сигурността за тяхната защита.

**Политика за използване на мрежовите услуги**

В дружеството е формулирана политика, отнасяща се до използването на мрежи и мрежови услуги.

Тя обхваща.

a) мрежите и мрежовите услуги, до които може да бъде даван достъп;
b) процедури за упълномощаване, за определяне на кого е разрешено да има достъп, за какви мрежи и за какви услуги;
c) видове контрол на управлението и процедури за защита на достъпа до мрежови връзки и мрежови услуги;
d) средства за контрол и процедури за ръководството, за да може то да защитава достъпа до мрежовите връзки и мрежови услуги.

Неразрешени и несигурни връзки към мрежови услуги могат да засегнат цялата организация на администрацията. Този контрол е особено важен за мрежови връзки към чувствителни или критични приложения или към потребители на високо рискови места, например обществени или външни области, които са извън управлението и контрола на сигурността на организацията.

**Оперативен контрол на достъпа до системите**

Прилагане на средства за сигурност на ниво операционна система, което ограничава достъпа до ресурсите на компютъра. Тези средства позволяват:

a) идентифициране и проверка на самоличността и ако е необходимо, терминалът или мястото на всеки упълномощен;
b) предоставяне на подходящи средства за определяне на самоличността; ако се използва система за управление на паролите, осигуряваща качествени пароли;

c) където е уместно, ограничаване на времето за връзка на потребителите.

**Контрол на достъпа до приложения**

Логическият достъп до софтуера и информацията е ограничен само до упълномощените потребители.

Приложните системи:

a) контролират достъпа на потребителите до информацията и до функциите на приложната система, в съответствие с определената политика за контрол на достъпа на бизнеса;
b) осигуряват защита срещу нерегламентирания достъп до всякакъв софтуер на служебни програми и на операционната система, който е в състояние да преодолее средствата за контрол на системата и на приложенията;
c) не излагат на риск сигурността на други системи, с които се използват съвместно информационните ресурси;
d) осигуряват достъп до информацията само за притежателя, за други определени упълномощени лица или за определени групи от потребители.

**Ограничение на достъпа до информация**

Когато е необходимо потребителите на приложни системи, включително персоналът по поддръжката, имат достъп до информацията и до приложните системи в съответствие с определена политика по контрол на достъпа, основана на изискванията на отделните бизнес приложения и съвместима с политиката на то за достъп до информацията.

Основните мерки за сигурност са:

a) предлагане на меню за контрол на достъпа до функциите на приложните системи;
b) ограничаване на знанията на потребителите за информация или за функции на приложни системи, за които те не са упълномощени да имат достъп, с подходящо редактиране на документацията, предназначена за потребителите;
c) контролиране на правата за достъп на потребителите, например, четене записване, изтриване или изпълнение;
d) осигуряване, че изходните данни от приложните системи, работещи с чувствителна информация, съдържат само информацията, която има отношение към използването на изходните данни и се изпращат само до упълномощени терминали и места, включително периодично преглеждане на такива изходни данни, за да се осигури, че излишната информация е отстранена.

**Изолиране на чувствителни системи**

Чувствителността на всяка приложна система е идентифицирана и документирана от притежателя на приложението, като към момента в „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД няма такива специфични случаи.

В дружеството са налични няколко основни мрежи – физически разделени една от друга, като управлението им е указано в „РАЗПРЕДЕЛЕНИЕ НА ИП мрежи в Топлофикация СФ“.

Разпределение на ИП мрежи в Топло

(Права на достъп: Системен администратор)

**Наблюдение на достъпа до системи**

Системите се наблюдават, за да се открият отклонения от политиката за контрол на достъпа и да се регистрират явления (процеси).

Наблюдението на системите позволява да се контролира ефикасността на приетите средства за контрол и да се провери съответствието с политиката по достъпа.

**Регистриране на събитията**

В дружеството се водят записи за изключения и други събития, отнасящи се до сигурността.

Те включват:

a) самоличности на потребителя;
b) данни и времена за влизане (регистриране) и излизане от системата;
c) идентификация на терминала и на местоположението, ако е възможно;
d) записи на успешни и на отхвърлени опити за достъп до системата;
e) записи на успешни и отхвърлени опити за достъп до данни и до други ресурси.

Записите/логовете се архивират в съответствие с политиката по запазване на записи или заради изискване за събиране на доказателства.

**Рискови фактори**

Резултатите от наблюдението се преглеждат редовно. Честотата на прегледите зависи от идентифицираните рискове. Отчитат се всичките рискови фактори, особено:

a) важността на приложния процес;
b) стойността, чувствителността и важността на информацията, за която става въпрос;
c) предишен опит от проникване в системата и злоупотреби;
d) обхватът на взаимно свързаността на системата.

**Регистриране и преглед на събитията (записи от видеонаблюдение)**

Прегледът на записите включва анализ на заплахите срещу системата и начинът, по който те могат да възникнат.

Средствата за контрол са насочени към защита срещу нерегламентирани изменения и проблеми при работа, включващи:

a) изключване на средството за водене на записи;
b) изменения във вида на съобщенията, които се записват;
c) редактиране или изтриване на записите;
d) препълване на носителя, на който се води записа и при това или не се прави запис на събитията или записът се презаписва върху себе си.

**Достъп до изходен код на програми**

Достъпът до програмни кодове е регламентиран и се управлява от ИКТ.

**Синхронизация на часовника**

Правилната настройка на часовниците на компютрите е важна, за осигуряване на точност на записите, предназначени за проверка, които са необходими за проучване или като доказателство в правни или дисциплинарни случаи.

==========

**(ПС-04)**

## УПРАВЛЕНИЕ НА ПАРОЛИ

Паролите са важен аспект от компютърната сигурност. Те са първата бариера за защита на потребителските акаунти. Неподходящо избрана парола може да доведе до компрометиране на компютърното оборудване в дружеството.

**Основни изисквания**

8. Всички пароли за достъп на системно ниво (например: root, enable, NT admin, application administration accounts, т.н.) трябва да бъдат променяни основно най – малко веднъж на тримесечие.

9. Всички пароли на потребителско ниво (например за: e-mail, web, персонален компютър, и т.н.) трябва да бъдат променяни задължително най-малко на всеки 6 (шест) месеца.

10. Потребителските акаунти, които имат права на системно ниво, разрешени посредством принадлежност в групи или програми, трябва да имат уникална парола, различаваща се от паролите за всички други акаунти притежавани от този потребител.

11. Паролите не трябва да бъдат вмъквани в E-mail съобщения или друга форма на електронна комуникация.

**Основни принципи при избора на парола**

Паролите се използват за различни цели. Някои от случаите, при които се използват пароли са: достъп до потребителските акаунти, E-mail акаунти и др. Тъй като много малко системи поддържат динамични пароли, които се използват еднократно, всеки трябва да знае как да избира сигурни пароли.

Несигурните, слабите пароли имат следните характеристики:

1. Паролата е съставена **от по-малко от 6 (шест) символа** – *задължително за изпълнение от всички потребители в дружеството!*
2. Паролата е дума съдържаща се в някакъв речник (Български, Английски или някакъв друг език);
3. Паролата е често използвана дума като:
4. Имена на роднини, приятели, колеги и др.
5. Компютърни термини, имена, команди, сайтове, фирми, хардуер, софтуер.
6. Производни на името на дружеството.
7. Рождени дати и друга лична информация, например адрес, телефонен номер, ЕГН и др.
8. Думи или цифрови последователности подобни на aaabbb, qwerty, zyxwvuts, 123321 и др.,
9. Някоя дума от преди това изброените записана в обратен ред.
10. Някоя дума от преди това изброените предхождана и ли следвана от цифра (например: secret1, 1secret).

Сигурните пароли имат следните характеристики:

14. Съдържат малки и големи букви (например: a-z, A-Z)
15. Съдържат цифри и пунктуационни символи, а също така и букви (например: 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
16. Представляват не по-малко от осем буквено – цифрова комбинация
17. Не са дума от някакъв език, диалект, жаргон и т.н.
18. Не се базират на лична информация, имена на роднини и т.н.
19. Паролите никога не трябва да се записват или съхраняват онлайн. Опитайте се да създавате пароли, които могат лесно да се запомнят. Един от начините да се постигне това е използването на заглавия на песни, сентенции и ли други фрази. Например фразата може да бъде "This May Be One Way To Remember", а паролата "TmB1w2R!" или "Tmb1W>r~" или някаква друга вариация.

*ЗАБЕЛЕЖКА: НЕ ИЗПОЛЗВАЙТЕ НИТО ЕДИН ОТ ГОРНИТЕ ПРИМЕРИ, КАТО ПАРОЛА!!!*

**Основни принципи за защита на паролите**

Не използвайте еднакви пароли за достъп до акаунтите в дружеството и за достъп до други акаунти не поддържани от дружеството (например: личен акаунт и др.). Където е възможно, не използвайте една и съща парола за достъп до различни системи. Например: изберете една парола за административната информационна система и отделна парола за ИТ системите.

***НЕ СПОДЕЛЯЙТЕ ПАРОЛИТЕ С НИКОГО, ВКЛЮЧИТЕЛНО И С КОЛЕГИТЕ СИ.***

***ВСИЧКИ ПАРОЛИ ТРЯБВА ДА БЪДАТ РАЗГЛЕЖДАНИ КАТО ЧУВСТВИТЕЛНА, ПОВЕРИТЕЛНА ИНФОРМАЦИЯ ЗА ДРУЖЕСТВОТО*!**

СПИСЪК ОТ ЗАБРАНИ:

4. Не съобщавайте паролата си по телефона на НИКОГО!
5. Не изпращайте паролата си в E-mail съобщения!
6. Не разкривайте паролата си дори на прекия си ръководител!
7. Не говорете за паролата си пред другите!
8. Не загатвайте за формата на паролата си (например: моята фамилия)!
9. Не разкривайте паролата си във въпросници или формуляри по сигурността!
10. Не споделяйте паролата си със членовете на семейството си!
11. Не разкривайте паролата си на колеги за периода, докато сте в отпуск!

Ако някой от колегите Ви поиска паролата, препратете ги към този документ или им кажете да се обадят на Изпълнителния директор.

Не използвайте възможността "Remember Password" (запомняне на парола) на програми като OutLook, MOZILLA FIREFOX, INTERNET EXPLORER и др.

И отново не записвайте паролите си и не ги съхранявайте на работното място. Не съхранявайте паролите си във файл на НИКАКВА компютърна система (включително джобни компютри или мобилни телефони и устройства) без криптиране.

Променяйте паролите си най-малко веднъж на шест месеца (освен паролите за системен достъп, който трябва да се променят на тримесечие). Препоръчителният интервал за смяна на паролите е четири месеца.

Ако има предположение, че даден акаунт или парола са компрометирани, съобщете на системния администратор и променете всички пароли.

*ЗАБЕЛЕЖКА*: Разбиване или разгадаване на парола може да бъде извършвано за служебни нужди периодично или на случайни периоди от време от Системния администратор. *Ако паролата е разгадана или разбита по време на тези сканирания, потребителя ще бъде помолен да промени паролата си.*

==========

**(ПС-05)**

## ВЗАИМООТНОШЕНИЯ С ВЪНШНИ СТРАНИ И ДОСТАВЧИЦИ

Настоящата политика отчита категоризациите на информацията, правните и договорни изисквания и съответните рискове.

1. Контактът с клиенти се извършва посредством задължително придружаване от страна на представител на «ТОПЛОФИКАЦИЯ СОФИЯ» ЕАД. Не се дава достъп до информация на хартиен носител или в електронен вид, която не е за обществено ползване. Не се предоставят на клиентите чужди лични данни и тайни. Периметърът на административните сгради на дружеството е под постоянно видеонаблюдение.
2. Достъпът на външни страни до чувствителна и критична информация или до активите се допуска само в присъствието и под контрола на компетентен служител на дружеството и след подписване на декларация за конфиденциалност.
3. Физическа зона за паркиране е с постоянно видеонаблюдение и под наблюдението на 24-часовата физическа охрана. При необходимост от доставки извън тази зона, доставящите влизат само в присъствието и под контрола на дежурния на смяна служител на дружеството.
4. В договори/анекси с външни страни се включват клаузи за конфиденциалност.

==========

**(ПС-06)**

## ИЗПОЛЗВАНЕ НА МРЕЖОВИ УСЛУГИ И НОСИТЕЛИ

Неразрешени и несигурни връзки към мрежови услуги могат да засегнат цялата организация. Този контрол е особено важен за мрежови връзки към чувствителни или критични бизнес приложения или към потребители на високо рискови места, например обществени или външни области, които са извън управлението и контрола на сигурността на общината.

За ограничаване на достъп само до услугите, за които са специално упълномощени да използват, се прилагат следните правила:

1. Достъп до мрежите и мрежовите услуги се разрешава за потребител само след разрешение от ИКТ по заявка от съответния ръководител на структурното звено;
2. Осигурява се достъп след съгласуване на кого е позволено да има достъп и до кои мрежи и мрежови услуги;
3. Контрол на управлението и за защита на достъпа до мрежови връзки и мрежови услуги се извършва чрез осигурен от системен администратор достъп за потребител на конкретна компютърна конфигурация.
4. Средствата, използвани за достъп до мрежи и мрежови услуги, се контролират от системен администратор.
5. Външен достъп до мрежи или мрежовите услуги се осъществява по условията на договор с външната организация.

**Боравене с носители**

Управление на сменяеми носители

Сменяемите носители включват дискове, флаш памети, сменяеми твърди дискове, CD, DVD и печатни носители.

1. ако повече не са необходими, съдържанията на всякакви повторно използваеми носители, които трябва да бъдат изнесени от дружеството, се изтриват от приносителя им;
2. всички носители се съхраняват в безопасна сигурна среда в съответствие със спецификациите на производителите или в шкафове от ползвателите им или съхраняващите ги;
3. запомнената информация върху носителите, която трябва да е достъпна по-дълго време, отколкото е животът на носителя (в съответствие със спецификациите на производителите), се записва на сървър от системен администратор за компютърна информация и от съхраняващите ги чрез копия при печатни носители, за да се избегне загуба на информация, поради разваляне на носителя
4. носителите за компютърна информация се предоставят от отдел техническо осигуряване по заявка от ползвателите.
5. В случай на получено разрешение и изнасяне на носители извън физическите граници на дружеството, те се поставят в подходяща опаковка и в надписан и запечатан плик

За предпазване от заразяване с вируси, за сменяемите информационни носители се прилага програмна защита при всяко поставяне в компютър.

Заразените устройства се изчистват от вируси или се изтриват заразените файлове.

**Унищожаване на носители, работа с информацията**

След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица, като се прилага следната процедура:

1. носители, съдържащи чувствителна информация, се съхраняват и унищожават чрез нарязване на хартиения

носител, за което отговаря ръководител отдел
2. изпразнени от данни сменяеми носители със системна информация се ползват за други приложения в дружеството, за което отговаря системен администратор;
3. извършва се избор на подходящ доставчик с достатъчни видове контрол и опит за събиране и унищожаване на хартия, устройства и носители;
4. физическото унищожаване на информационните носители (CD-дискове и дискети) става със счупване. Предварително се проверят, за да е сигурно, че цялата информация е изтрита от тях преди унищожаване.
5. при събиране на носители за унищожаване, се има предвид ефектът на струпване, който може да предизвика голямо количество нечувствителна информация да стане чувствителна.

==========

**(ПС-07)**

## МОБИЛНИ СРЕДСТВА И РАБОТА ОТ РАЗСТОЯНИЕ

Необходимата защита е пропорционална на рисковете, причинени от тези специфични методи за работа. Когато се използва преносим компютър, трябва да се вземат предвид рисковете при работа в незащитена среда и да се приложи подходяща защита. В случай на работа извън централния офис трябва да се прилагат защита на мястото, където работи и да осигури, че са взети подходящи мерки за този начин на работа и невъзможност от кражба на информация или на хардуерното устройство.

**Мобилна работа с компютър или друго мобилно устройство.**

Когато се използват преносими компютри (ноутбук, палмтоп, лаптоп и мобилни телефони) се вземат мерки за обезпечаване на сигурността на информацията. Преносимите компютри не се оставят без наблюдение.

Въведена е защита за избягване на нерегламентиран достъп до съхраняваната и обработвана от тези средства информация или разкриването и, например с използване на методи за шифроване. Резервните копия имат надеждна защита (срещу кражба или загубване на информацията).

Преносимите компютри трябва са физически защитени срещу кражба и не се оставят в коли или други форми на транспорт, хотелски стаи, зали за конференции и места за срещи. Оборудване, съдържащо важна, чувствителна и / или с критично значение информация, не се оставя без надзор и когато е възможно е физически заключено на скришно място или се използват специални ключалки за обезопасяване на оборудването.

Организирано е обучение за персонала, използващ преносими компютри, за да се повиши осъзнаването от тяхна страна на допълнителните рискове.

**Работа от разстояние**

Осъществяване на свързване посредством правилата на домейн контролер, парола, Vpn-ipSEC.

==========

**(ПС-08)**

**КОМУНИКАЦИИ С ЕЛЕКТРОННА ПОЩА**

За нуждите на „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД се използват само и единствено служебни електронни адреси.

Всички електронни адреси в дружеството се генерират в следния порядък:

**x.yyyyyyyy@toplo.bg,**

където „x“ – първата буква от името на притежателя

„yyyyyyyyy” – фамилията на притежателя

В случай на необходимост се допуска добавяне на допълнителни букви или символи за избягване на повтаряемост.

Задължителен атрибут към всеки E-mail е поставянето на идентификатора на притежателя на пощата съгласно заповед на Изпълнителния директор.

**ЗАБРАНИ:**

- ⇨ Комуникиране посредством електронната поща с цел различна от изпълнение на служебните задължения и не свързана с функционалните характеристики на притежателя.
- ⇨ Работа с електронна поща (отваряне, сваляне и записване на файлове на PC) без включена активна антивирусна защита.
- ⇨ Изпращане на нежелани E-mail съобщения включително изпращането на "junk mail" или други рекламни материали към реципиенти, които изрично не са заявили такива материали (E- mail spam).
- ⇨ Всякакъв вид на тормоз посредством E- mail, телефон или др. било то посредством говор, честота на повтаряне или размер на съобщенията.
- ⇨ Неправомерното използване или подмяна на хедър информацията в E- mail съобщенията.
- ⇨ Искане на E-mail съобщения за E-mail адреси различни от този, с който се е представил съответния акаунт с цел тормоз или събиране на отговори.
- ⇨ Създаване или препредаване на “верижни писма” или E- mail съобщения по други “пирамидални” схеми.
- ⇨ Използване на E- mail съобщения за разпространение на оферти в полза на други организации или за реклама и предлагане на услуги хоствани от дружеството или достъпни посредством неговата мрежа.
- ⇨ Изпращане на същите или подобни съобщения, които нямат връзка с дейността на „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД към голям брой членове на нюзгрупи (newsgroup spam).

==========

**(ПС-09)**

**КРИПТОГРАФСКИ МЕХАНИЗМИ ЗА КОНТРОЛ**

Криптографските методи и средства са съвкупности от криптографските механизми, чиито основни елементи са криптографските алгоритми.

Опазването на секретните ключове от нерегламентиран достъп е от основно значение за сигурността на защитаваната информация, поради което се отделя специално внимание на съхранението им.

В „ТОПЛОФИКАЦИЯ СОФИЯ“ ЕАД се използват вградени политики на съответните хардуерни устройства, използване на VPN свързаност и правилата регламентирани от “domain controller”.

| | |
|---|---|
| **ДИСЦИПЛИНАРЕН КОНТРОЛ:** | ЗАДЪЛЖЕНИЕ НА ВСЕКИ КОМПЮТЪРЕН ПОТРЕБИТЕЛ Е ДА ЗНАЕ ТЕЗИ ОСНОВНИ ПРИНЦИПИ И ДА ГИ ПРИЛАГА ПРИ СВОЯТА ДЕЙНОСТ.<br><br>ВСЯКО ДЛЪЖНОСТНО ЛИЦЕ НАРУШИЛО ТЕЗИ ПОЛИТИКИ МОЖЕ ДА Е ОБЕКТ НА ДИСЦИПЛИНАРНО НАКАЗАНИЕ, ВКЛЮЧИТЕЛНО И ДИСЦИПЛИНАРНО УВОЛНЕНИЕ. |