Infinity - Head office
36 blvd. Dragan Tsankov
Interpred - WTC Sofia 1040
tel.: +359 2 489 02 60
GSM: +359 888 626423
e-mail: office@infinity.bg
www.infinity.bg

Решения за информационна сигурност от Инфинити ООД

- **Постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност**

✓ **Класификация на информацията**	Технологична област	Техническо решение
Чл. 6. (1) Субектът приема вътрешни правила по смисъла на чл. 5, ал. 1, т. 6 и 7 за класификация на информацията, които указват как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага организацията. Препоръчителна класификация е дадена в приложение № 2.	▪ Data Classification & Labeling	▪ BoldonJames

✓ **Управление на информационните активи**	Технологична област	Техническо решение
Чл. 8. (1) Субектът приема вътрешни правила по смисъла на чл. 5, ал. 1, т. 6, регламентиращи процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти. Вътрешните правила трябва еднозначно да указват условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти. (2) Описът на информационните активи по смисъла на чл. 5, ал. 1, т. 1 съдържа информация, необходима за разрешаването на инциденти, анализ и оценка на риска, управление на уязвимости и управление на измененията ...	▪ Device Visibility ▪ Device Control ▪ Data Leak Prevention - DLP ▪ Asset Management ▪ Certified Secure Data Erasure	▪ Cososys - Endpoint Protector ▪ DeviceLock ▪ Vicarius Topia ▪ Blancco

✓ **Управление на взаимодействията с трети страни**	Технологична област	Техническо решение
Чл. 10. (1) При установяване на взаимоотношения с доставчици на стоки и услуги, наречени „трети страни“, Субектът трябва да договори изисквания за мрежова и информационна сигурност ... (2) Субектът определя служител/служители, отговарящ/отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване. (3) Субектът изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.	▪ Privileged Access Management ▪ Privileged User Monitoring ▪ Sessions Monitoring ▪ Recording and Management	▪ SSH Communications PrivX

Infinity - Head office
36 blvd. Dragan Tsankov
Interpred - WTC Sofia 1040
tel.: +359 2 489 02 60
GSM: +359 888 626423
e-mail: office@infinity.bg
www.infinity.bg
Distributor & Value Added Reseller

✓ **Неоторизирано използване на устройства**	Технологична област	Техническо решение
Чл. 15. (1) Субектът приема ясно дефинирани политики относно използването на: 1. лични технически средства в мрежата, която контролират; 2. преносими записващи устройства. (2) Политиките се отразяват във вътрешните правила, като се предприемат подходящи и реципрочни на заплахите мерки за реализирането им.	▪ Device Visibility ▪ Device Control ▪ Data Leak Prevention	▪ Cososys - Endpoint Protector ▪ DeviceLock ▪ DataLocker

✓ **Криптография**	Технологична област	Техническо решение
Чл. 16. (1) Субектът разработва политика и вътрешни правила съгласно чл. 5, ал. 1, т. 6 за прилагане на криптографски механизми, които се използват за гарантиране на конфиденциалността и интегритета на чувствителната информация в съответствие с нейната класификация. (2) Криптографските механизми се съобразяват с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритет и с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.	▪ Encryption	▪ DataLocker ▪ Iron Key ▪ GalaxKey ▪ EasyLock

✓ **Защита на софтуер и фърмуер**	Технологична област	Техническо решение
Чл. 22. (1) Субектът инсталира и поддържа само версии на използвания в системите му софтуер и фърмуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността. (2) Административният орган, съответно ръководителят на субекта по чл. 1, ал. 1, т. 2 – 5, одобрява софтуера, който се използва в информационните и комуникационните системи. (3) Субектът поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер с цел намаляване на времето за възстановяване на дадена система след срив. (4) Субектът предприема мерки за: 1. недопускане на инсталирането и използването на неодобрен софтуер и фърмуер; 2. контрол върху използвания софтуер и фърмуер, включително неговата актуалност. (5) Субектът приема вътрешни правила и инструкции за регламентиране на действията ...	▪ Vulnerability Management ▪ Automatic and Manual Patching ▪ Backup	▪ Vicarius Topia ▪ Actiphy (NetJapan)

Infinity - Head office
36 blvd. Dragan Tsankov
Interpred - WTC Sofia 1040
tel.: +359 2 489 02 60
GSM: +359 888 626423
e-mail: office@infinity.bg
www.infinity.bg
Distributor & Value Added Reseller

✓ **Защита от зловреден софтуер**	Технологична област	Техническо решение
Чл. 23. (1) Субектът прилага в информационната и комуникационната си инфраструктура подходящи мерки за защита от проникване и мерки за откриване и справяне със зловреден софтуер. (2) Мерките за защита от зловреден софтуер трябва ...	▪ Endpoint Protection ▪ Vulnerability Management ▪ Automatic and Manual Patching	▪ Avira ▪ Vicarius Topia

✓ **Защита на индустриални системи за контрол**	Технологична област	Техническо решение
Чл. 27. В случай че Субектът използва индустриални системи за контрол, от функционирането и сигурността на които зависят съществените услуги, които предоставя, той е задължен да приложи подходящи мерки за тяхната защита в съответствие с изискванията на наредбата, ако са приложими.	▪ Vulnerability Management ▪ Automatic and Manual Patching ▪ Backup ▪ Device Visibility ▪ Device Control ▪ Data Leak Prevention ▪ Certified Secure Data Erasure ▪ Privileged Access Management ▪ Privileged User Monitoring ▪ Sessions Monitoring ▪ Recording and Management	▪ Vicarius Topia ▪ Actiphy (NetJapan) ▪ Cososys - Endpoint Protector ▪ DeviceLock ▪ Data Locker ▪ Blancco ▪ SSH Communications PrivX

✓ **Наблюдение**	Технологична област	Техническо решение
Чл. 28. (1) Субектът използва система/системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността му системи, чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства, позиционирани така, че да могат да анализират всички потоци, обменяни между собствените им информационни и комуникационни системи, както и с информационните и комуникационните системи на трети страни. (2) Субектът организира чрез вътрешни правила и/или инструкции действията за наблюдение и реакция на сигналите от тази/тези система/системи.	▪ Threat Detection ▪ Security Intelligence ▪ Asset Management ▪ SIEM and Log Management ▪ Vulnerability Assessment ▪ Intrusion Detection System ▪ Compliance	▪ AlienVault - AT&T Cybersecurity

Infinity - Head office
36 blvd. Dragan Tsankov
Interpred - WTC Sofia 1040
tel.: +359 2 489 02 60
GSM: +359 888 626423
e-mail: office@infinity.bg
www.infinity.bg

✓ **Системни записи (logs)**	Технологична област	Техническо решение
Чл. 29. По отношение на системните записи Субектът гарантира ...	▪ Threat Detection ▪ Security Intelligence ▪ Asset Management ▪ SIEM and Log Management ▪ Vulnerability Assessment ▪ Intrusion Detection System ▪ Compliance	▪ AlienVault - AT&T Cybersecurity

✓ **Управление на инциденти с мрежовата и информационната сигурност**	Технологична област	Техническо решение
Чл. 30. (1) Във вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 се регламентират всички дейности при обработката на сигнали и реакция при инциденти ...	▪ Threat Detection ▪ Security Intelligence ▪ Asset Management ▪ SIEM and Log Management ▪ Vulnerability Assessment ▪ Intrusion Detection System ▪ Compliance	▪ AlienVault - AT&T Cybersecurity

✓ **Уведомяване за инциденти**	Технологична област	Техническо решение
Чл. 31. (1) При инцидент с мрежовата и информационната сигурност служителят или административното звено, отговарящо за мрежовата и информационната сигурност по смисъла на чл. 3, ал. 2, уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност ...	▪ Threat Detection ▪ Security Intelligence ▪ Asset Management ▪ SIEM and Log Management ▪ Vulnerability Assessment ▪ Intrusion Detection System ▪ Compliance	▪ AlienVault - AT&T Cybersecurity

✓ **Резервиране и архивиране на информация**	Технологична област	Техническо решение
Чл. 32. (1) Вътрешните правила/инструкции по смисъла на чл. 5, ал. 1, т. 6 се разработват в съответствие с целите и стратегическите насоки, определени в политиката за мрежова и информационна сигурност относно защита на интегритета на информацията в случай на инцидент, засягащ нейната достъпност ...	▪ Backup	▪ Actiphy (NetJapan)

Infinity - Head office
36 blvd. Dragan Tsankov
Interpred - WTC Sofia 1040
tel.: +359 2 489 02 60
GSM: +359 888 626423
e-mail: office@infinity.bg
www.infinity.bg

Enterprise IT Security solutions

Distributor & Value Added Reseller

DeviceLock · blancco · boldonjames · DataLocker · galaxkey · observe it · clearswift · COSOSYS · NetJapan · IRONKEY · ENDPOINT PROTECTOR · handheld · CYCLOPE · ALIEN VAULT · Vicarius

✓ КЛАСИФИКАЦИИ НА ИНФОРМАЦИЯТА	Технологична област	Техническо решение
С цел да се гарантира достатъчна, адекватна и пропорционална на заплахите защита на информацията, се прави преценка на важността и чувствителността ѝ, както и на нормативните изисквания към нея. Въз основа на тази преценка информацията се разделя в няколко категории. Когато е приложимо, тази класификация се пренася и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето, разпространението и унищожаването на информацията, и към тях се прилагат подходящи мерки за защита, съответстващи на заплахите ...	▪ Data Classification & Labeling ▪ Data Leak Prevention - DLP	▪ BoldonJames ▪ Cososys - Endpoint Protector ▪ DeviceLock

✓ ИЗИСКВАНИЯ ЗА КОНФИГУРИРАНЕ	Технологична област	Техническо решение
1. Да се забрани macros в office пакетите. 2. Да се забрани pop-up в браузерите. 3. Auto play функцията да се конфигурира винаги да иска потвърждение на потребителя. 4. User Account Control да се конфигурира до най-високо ниво, така че винаги да издава предупреждения. 5. При споделянето на файлове и принтери да не се използва настройка Everyone, а да се указва кои акаунти точно да имат право на достъп до тях. 6. Да се забрани TRACE/TRACK методът. 7. Да се забрани anonymous authentication. 8. Да се използва Unicast Reverse-Path Forwarding (uRPF) за предпазване от използването на фалшиви IP адреси и rate-limiting за ограничаване на броя на заявките по IP адрес. 9. Да се забрани TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия. 10. Съобщенията за грешки в системите да не дават излишна информация. 11. Да не се използва AutoComplete. 12. Да се използват приложения (add-ons) към браузърите за блокиране на рекламно съдържание.	▪ Endpoint Protection	▪ Active Directory Avira

- Тази таблица посочва продукти, свързани с наредбата за минималните изисквания за мрежова и информационна сигурност.
- Това не са всички продукти, а само тези, с които Инфинити ООД най-усилено работи и има високи партньорски нива.
- Продуктите, посочени в таблицата, сами по себе си не изпълняват изискванията изцяло, а подпомагат или улесняват решаването на проблемите. Наличието на съответните процедури, документация и административни мерки са голяма част от изискванията на наредбата.