



Политика за информационна сигурност

Съдържание:

1. Въведение	3
За компанията	3
1.1. Цел	3
1.2. Обхват	4
1.3. Съответствие с регулаторните изисквания	5
2. Управление на активи	6
3. Контрол срещу зловреден софтуер	8
4. Управление на техническите уязвимости	8
5. Архивиране на информация	10
6. Резервиране на ресурси за обработка на информация	11
7. Регистриране и наблюдение на събития	11
8. Механизми за мрежов контрол	15
9. Сигурност на мрежовите услуги	16
10. Филтриране на уеб съдържание	17
11. Управление на промените	18
12. Контрол на достъпа и управление на самоличността	19
13. Управление и докладване на инциденти	20
14. Роли и отговорности	22
15. Обучение и осведоменост	23
16. Преглед и актуализации	24
17. Непрекъснато усъвършенстване	24
18. Връзка с други документи	25

1. Въведение

За компанията

„Бони Холдинг“ е най-големият производител на свинско месо в България и ключов играч в хранително-вкусовата промишленост, доставяйки 30% от прясното свинско месо в страната. Компанията се фокусира основно върху свиневъдството и преработката на месо, допълнени от производството на фуражи, които подпомагат развъдната ѝ дейност.

Ние управляваме седем свинеферми за отглеждане на добитък и разполагаме с три съоръжения за производство на фуражи, предназначени за нашите животни. Основният ни център за преработка на месо се намира в Ловеч и включва индустриална транжорна, фабрика за производство на салами и деликатеси и фабрика за производство на месни заготовки (месни разфасовки, кайма, сурови колбаси и полуфабрикати; готови за консумация/готвене продукти). Близостта на тези три предприятия създава високоефективен производствен комплекс.

Освен това, разполагаме с уникално съоръжение за сурово-сушени продукти в Карлово, известно със специализираната си микросреда, която придава отличителен вкус на нашите продукти. През 2021 г. подобрихме нашия бизнес модел, като открихме най-технологично напредналата кланица за свине в България в Търговище, която играе жизненоважна роля за осигуряване на високото качество на нашите животни по цялата верига за преработка на месо.

Чрез нашите фуражни заводи, свинеферми и месопреработвателни предприятия, ние гарантираме, че нашите продукти отговарят на най-високите стандарти за качество, като същевременно допринасяме положително за българската икономика и общество. Нашата мисия е да осигуряваме на българите отговорно произведено месо, като гарантираме грижа за хората, животните и околната среда. За да постигнем това, сме си поставили четири стратегически цели, които да оформят развитието на компанията през следващите години и след това:

- Увеличаване на дела на свинското месо, произведено в България, в общото потребление на българите (в момента две трети от консумираното свинско месо идва от Европа).
- Утвърждаване на лидерската ни позиция и превръщането ни във водещи новатори в месопреработвателната индустрия.
- Задоволяване на нуждите на нашите клиенти чрез нашето мащабно производство и способността ни да контролираме повече етапи от производството.
- Поддържане на имиджа на месото като основна храна и насочване на усилията към популяризиране на неговото значение.

1.1. Цел

Тази Политика за информационна сигурност на Бони Холдинг е основополагащ документ, който определя рамката и принципите за защита на информацията и мрежовите активи на организацията.

Целта на политиката за информационна сигурност е да:

- Защити активите, мрежите и системите от инциденти, загуба на данни, неоторизиран достъп и прекъсвания.
- Осигури непрекъснатост на критични бизнес процеси, особено в производството и логистиката.
- Установи ясни роли, отговорности и процедури за предотвратяване, откриване и реагиране на инциденти, свързани със сигурността.
- Приложи подходящи технически и организационни мерки.
- Повиши осведомеността и културата за информационната сигурност сред всички служители и партньори.

1.2. Обхват

Тази политика се прилага за всички подразделения и предприятия в структурата на Бони Холдинг:

Направление „Свиневъдство“:

- Бони Ферма Брестак АД
- Бони Ферма Крумово Градище АД
- Бони Ферма Зимен АД
- Бони Ферма Никола Козлево АД
- Бони Ферма Шумен АД
- Бони Ферма Левски АД
- Бони Ферма Плевен АД
- Бони Фуражи Пордим ЕООД

Направление „Месопреработка“:

- Бони Месокомбинат Ловеч АД
- Бони Месокомбинат Карлово АД
- Бони Месокомбинат Русе АД

- Бони Маркетинг ЕООД

Политиката за информационна сигурност се прилага и за:

- Всички ИТ и комуникационни системи, разположени на територията на България, включително 17-те оперативни обекта на компанията.
- Всички служители, външни изпълнители и доставчици, които имат достъп до системи и/или данни.
- Всички активи, включително сървъри, работни станции, мрежови устройства, софтуерни системи, камери за наблюдение и контролери (включително ERP и DVR системи).
- Всички процеси, свързани с управление на достъпа, реагиране при инциденти, архивиране на данни, системни актуализации, обучение и други съответни дейности.

1.3. Съответствие с регулаторните изисквания

Политика за информационна сигурност на Бони Холдинг е разработен в съответствие с приложимата правна рамка в областта на мрежовата и информационната сигурност, включително, но не само:

1.3.1 Европейско законодателство

- Директива (ЕС) 2022/2555 (NIS2) – относно мерки за високо общо ниво на киберсигурност в Съюза. Тази директива разширява обхвата на регулираните субекти и засилва изискванията за управление на риска и докладване на инциденти.
- Регламент (ЕС) 2016/679 (GDPR) – относно защитата на личните данни и неприкосновеността на личния живот.
- Регламент (ЕС) 910/2014 (eIDAS) – относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

1.3.2 Национално законодателство

- Закон за киберсигурността (обнародван в ДВ бр. 94/2018 г.), актуализиран за транспониране на Директивата NIS2. Той въвежда нови категории обекти („съществени“ и „важни“) и налага по-строги мерки за киберсигурност и задължения за докладване на инциденти.
- Наредба за минималните изисквания за мрежова и киберсигурност (MRNIS) – приложима за операторите на основни услуги, определяща както организационни, така и технически стандарти за сигурност.
- Закон за защита на личните данни – хармонизиране на националните практики за защита на данните с GDPR.
- Наказателния кодекс и Закона за електронното управление – особено в разделите, отнасящи се до ИТ инциденти и злоупотреба с данни.

1.3.3. Най-добри практики и международни стандарти

Политиката е в съответствие и с препоръките на международно признати стандарти и насоки, включително:

- ISO/IEC 27001 – Системи за управление на сигурността на информацията (СУСИ)
- ISO/IEC 27005 – Управление на рисковете за сигурността на информацията
- ISO 22301 – Системи за управление на непрекъснатостта на дейността
- ENISA (Агенция на Европейския съюз за киберсигурност) – Насоки и препоръки за прилагане на NIS2

Политиката се прилага под надзора на Министерството на електронното управление (МЕУ), определено за компетентен орган за прилагане на изискванията на NIS2 за основни субекти в сектора „Производство и преработка на храни“.

2. Управление на активи

2.1. Дефиниции

Актив е всеки елемент, който има стойност за „Бони Холдинг“ и може да бъде обект на киберзаплахи, включително:

- Хардуер: Компютри, сървъри, мрежово оборудване (защитни стени, комутатори, рутери), DVR устройства, контролери, принтери, камери и др.
- Софтуер: Операционни системи (Windows, Windows Server), ERP системи, Microsoft 365, SIEM (Rapid7), антивирус (ESET), Veeam и др.
- Данни: Информация за клиенти, производство, търговия, човешки ресурси и финанси.
- Услуги: Облачни платформи, имейл системи, отдалечен достъп, външни API и др.

2.2. Видимост и контрол

Ефективната защита на информационната и оперативната инфраструктура на Бони Холдинг изисква пълна видимост върху всички активи – хардуер, софтуер, мрежови компоненти и информационни ресурси. Този раздел определя процедурите и отговорностите за управление на активите.

2.3. Механизми за контрол

Изборът на механизми за технологичен контрол следва клауза 8 от приложение А на ISO/IEC 27001:2022. Внедряването взема предвид законови, регулаторни, договорни и други изисквания, за да се осигури високо ниво на сигурност на информацията и съответствие на системите за управление на сигурността на информацията (СУСИ) със стандарта.

2.4. Правила за устройствата на крайните потребители

Тази политика се отнася за всички служители и обхваща всички устройства за обработка на данни, използвани редовно в дейността. Тези устройства, когато са свързани към системите и мрежите на „Бони Холдинг“, попадат в обхвата на тази политика, за да се гарантира защитата на всяка информация, съхранявана, обработвана или достъпвана чрез тях.

2.5. Правила за устройствата, собственост на компанията

Политиката обхваща всички видове стационарни и мобилни компютри, собственост на „Бони Холдинг“. Ключовите разпоредби включват:

- Физическа сигурност: Устройствата не трябва да се оставят без надзор на небезопасени места, в обществен или частен транспорт или на работни места без надзор.
- Потребителски акаунти: Достъпът до устройствата трябва да се осъществява чрез лични акаунти, за да се осигури сигурно удостоверяване и оторизация.
- Резервни копия: „Бони Холдинг“ не поддържа резервни копия на лични компютри или мобилни устройства.
- Криптиране: Всички мобилни компютри трябва да използват криптирани файлови системи.
- Ограничения на достъпа: Служителите нямат право да предоставят устройствата си на трети страни или да инсталират/изтеглят неоторизирано съдържание или приложения.
- Политика за чист екран: Служителите трябва да заключват екраните, когато не се използват, и да предотвратяват сърфирането през рамо.
- Съхранение на информация: За бизнес данни е осигурено защитено хранилище. По подразбиране никакви бизнес данни не трябва да се съхраняват локално на устройствата на крайните потребители, за да се предотврати неоторизирано разкриване или загуба.
- Лични данни: Съхраняването на лични или защитени с авторски права данни на фирмени устройства е забранено.
- Достъп до мрежата: Устройствата, които не са част от домейн групата, нямат право да се свързват с вътрешната мрежа.
- Операционни системи: Допускат се само версии на операционни системи, поддържани от производителя. Могат да се използват множество поддържани версии в зависимост от лицензирането, капацитета на хардуера или възможността за надграждане.
- Периферни устройства: Използването на USB устройства, преносими интернет карти и други аксесоари не е забранено.

- Функции за сигурност: Където е технически възможно, устройствата трябва да използват UEFI boot и TPM 2.0. TPM 2.0 е задължителен за всички придобивания на нов хардуер.

3. Контрол срещу зловреден софтуер

3.1. Общ подход

„Бони Холдинг“ внедрява ефективни инструменти и механизми за откриване и защита от зловреден софтуер, както и подходящи процедури за поддържане на високо ниво на сигурност. Защитата се основава на:

- Осведоменост за сигурността
- Контролиран достъп до системите
- Утвърдени практики за управление на промените

3.2. Внедрени механизми за контрол

Дружество „Бони Холдинг“ е предприело следните мерки за защита срещу зловреден софтуер:

- Интегрирана антивирусна програма и внедряване на технологията за киберсигурност EDR: Цялостна комбинация от ESET Antivirus и Rapid7 EDR се използва за прилагане на политики за сигурност, централизирано управление, сканиране, контрол на приложения, контрол на преносими устройства и наблюдение на мрежовия трафик.
- Сканиране на файлове: Всички прикачени файлове към имейли и изтеглени файлове се сканират за злонамерен софтуер преди употреба. Това сканиране се извършва на множество места: имейл шлюзове, сървърни системи, настолни и мобилни компютри и когато съобщенията влязат в мрежата на „Бони Холдинг“.
- Периодични системни сканирания: Информационните системи, частично или изцяло, се сканират редовно за злонамерен софтуер.
- Защита от несанкциониран достъп: Не е възможно да се деактивират интегрираните софтуерни продукти, отговорни за откриването и защитата от зловреден софтуер.

4. Управление на техническите уязвимости

4.1. Насоки за управление на технически уязвимости

За да се осигури ефективен контрол, се следват следните процедури, когато се установи потенциална техническа уязвимост:

- Отговорност на трета страна: „Бони Холдинг“ е назначила трета страна партньор с отговорности за управление на уязвимостите, включително мониторинг, оценка на риска, отстраняване на проблеми, проследяване на активи и координация.
- Инструменти и осведоменост: Инструменти като Rapid7 InsightVM и ESET се използват за идентифициране на уязвимости и поддържане на осведоменост.
- Реакция на предупреждения: Организацията може да реагира на предупреждения за новооткрити уязвимости чрез външния Оперативен център за защита (SoC), вътрешни ИТ екипи или бюлетини за сигурност.
- Оценка на риска и отстраняване: При откриване на потенциална уязвимост, външният Оперативен център за защита (SoC) оценява свързаните рискове и инициира коригиращи действия.
- Реакция, основана на спешност: Действията се приоритизират въз основа на спешността и сериозността на уязвимостта, в съответствие с изискванията за сигурност.
- Актуализации на софтуера: Рисковете, свързани с актуализациите на софтуера, се оценяват. Актуализациите се тестват и оценяват преди внедряването им в производствена среда.
- Алтернативни контроли: Ако няма налични актуализации или корекции на фърмуера, се прилагат алтернативни контроли:
 - Деактивиране на уязвими услуги или функции
 - Преконфигуриране или добавяне на механизми за контрол на достъпа
 - Подобряване на мониторинга за откриване или предотвратяване на атаки
 - Повишаване на осведомеността за специфичната уязвимост
- Одитни следи: За определени процедури се поддържат контролни записи.
- Непрекъснатата оценка: Процесът на управление на уязвимостите се наблюдава и оценява редовно, за да се гарантира неговата ефективност.

4.2. Редовна инвентаризация

Всички заинтересовани страни – включително вътрешният екип на „Бони Холдинг“, доставчиците на ИТ услуги и външният Оперативен център за защита (SoC) – провеждат редовни инвентаризации на активите, за да поддържат приемливи нива на техническа уязвимост.

4.3. Мониторинг на съответствието със сигурността

Спазването на изискванията за сигурност се следи от външния Оперативен център за защита (SoC) в тясно сътрудничество с техническите експерти на „Бони Холдинг“.

4.4. Оценка на сигурността на нови системи

Преди внедряването на нови информационни системи или техническо оборудване, Бони Холдинг оценява функциите за сигурност, предоставени от производителя. Решение за внедряване се взема само ако са спазени необходимите нива на сигурност.

4.5. Проверки за уязвимости след внедряване

След внедряването, външният Оперативен център за защита (SoC) извършва периодични проверки, за да идентифицира уязвимости и заплахи. Констатациите се докладват на отговорния доставчик на услуги или на определен служител за отстраняване на проблемите.

5. Архивиране на информация

5.1. Стратегия за архивиране

Дружество „Бони Холдинг“ е внедрило подходящи механизми за архивиране, за да гарантира, че цялата критична информация и софтуер могат да бъдат възстановени след инцидент със сигурността. Процесът на архивиране и възстановяване включва:

- **Наличност на оперативни данни:** Оперативните данни, съхранявани и обработвани от системите, се архивират с помощта на различни технологии и места за съхранение, включително Veeam, NAS и Microsoft 365 Cloud. Поддържа се график за архивиране за системи, идентифицирани като важни или критични за бизнес операциите.
- **Съхранение на работни файлове:** Работните файлове от всички локални и преносими системи трябва да се запазват в Microsoft 365 или друга определена система. Файловете не трябва да се съхраняват на локални дискове на служителите. Служителите са инструктирани, че Бони Холдинг не може да гарантира наличността на файлове, които не се съхраняват в одобрени хранилища.
- **Контрол на достъпа:** Достъпът до резервни копия е строго контролиран.
- **Мониторинг на целостта:** Целостта и качеството на файловете, съхранявани в облачните услуги, се наблюдават с помощта на вградени механизми, за да се гарантира надеждност при извънредни ситуации.
- **Пълно възстановяване:** Методът на архивиране (бекъп) гарантира възстановяването на всички файлове, системни конфигурации и приложения.
- **Отговорност за възстановяване (бекъп):** Възстановяването се извършва от определения системен администратор или доставчик на услуги.
- **Тестване:** Резервните (бекъп) системи се тестват поне веднъж годишно чрез пробни възстановявания.

- ИТ системи на групата: Системите и данните, хоствани от вътрешни ИТ доставчици на групата, не подлежат на архивиране, тестване или управление от Бони Холдинг.

6. Резервиране на ресурси за обработка на информация

6.1. Анализ на единична точка на отказ

„Бони Холдинг“ провежда редовни анализи, за да идентифицира единични точки на отказ или системи, работещи с максимален капацитет. Ако бъдат открити такива проблеми, се предприемат незабавни действия за разрешаването им. Ако разрешаването не е осъществимо в рамките на текущия бюджетен цикъл, свързаният риск се документира и приема от ръководството.

6.2. Резервиране на облачна система

„Бони Холдинг“ използва облачни системи, чиято резервираност е гарантирана от доставчика на услуги. Ръководството е приело, че времето за работа на доставчика е достатъчно, за да отговори на изискванията за наличност. Тези облачни услуги обикновено поддържат географски разпределени реплики с автоматично пренасочване на трафика в случай на прекъсване на услугата. Този подход ефективно гарантира наличност и резервираност, когато е необходимо.

7. Регистриране и наблюдение на събития

7.1. Съхранение на дневника

Лог-файловете /дневниците/ на облачната платформа, които записват потребителски действия, изключения и нарушения на сигурността, се съхраняват за период от шест (6) месеца. Тези лог-файлове /дневници/ служат като доказателство в случай на разследвания и за наблюдение на контрола на достъпа.

7.2. Съдържание на лог-файловете /дневниците/

Контролните лог-файлове /дневници/ включват следната информация:

- Уникални потребителски имена или идентификатори
- Геолокация на всяко успешно влизане
- Дата, час и подробности за ключови събития (напр. стартиране/изключване на системата)
- Идентифициране на крайното устройство или местоположение, където е възможно
- Записи на успешни и отказани опити за достъп

- Записи на успешни и отказани опити за достъп до данни/ресурси
- Промени в системната конфигурация
- Използване на привилегировани акаунти
- Мрежови адреси и протоколи
- Активиране и деактивиране на модули за сигурност
- Неоторизирани изтегляния или споделяне на съдържание

7.3. Съхранение и анализ на лог файлове /дневници/

Всички регистрирани събития се съхраняват в защитени хранилища. „Бони Холдинг“ делегира управлението на виртуалното хранилище, контрола на съдържанието и анализа на лог файловете на външен Оперативен център за защита (SoC). Специалистите нямат право да изтриват, деактивират или променят записи в лог файловете.

Наблюдаваните области включват:

- Оторизиран достъп: Уникални потребителски идентификатори, времеви отпечатъци, типове събития, файлове, до които е осъществен достъп, и използвани приложения/инструменти
- Привилегировани операции: Използване на администраторски, специализирани или операторски акаунти; стартиране, рестартиране и изключване на системата
- Неоторизирани опити за достъп: Неуспешни или отхвърлени потребителски действия, нарушения на достъпа до данни/ресурси, нарушения на правилата за достъп, предупреждения от защитната стена и предупреждения от системата за откриване на прониквания.
- Промени в конфигурацията за сигурност: Опити за промяна на настройките за сигурност или механизмите за контрол

7.4. Защита на лог-файловете /дневниците/

Въведени са механизми за защита на данните от лог-файловете /дневниците/ от неоторизирано разкриване, промяна или изтриване. Ключовите защити включват:

- Ограничен достъп до лог-файловете /дневниците/
- Прегледът на съдържанието на лог файловете /дневниците/ е ограничен до системния мениджър и един определен специалист.

7.5. Регистриране на облачна платформа

Ръководството счита възможностите за регистриране на облачните платформи за достатъчни за проследяване на действията от системни администратори, специалисти и оператори. Тези регистрационни файлове включват:

- Времева маркировка на успешни или неуспешни събития
- Подробности за събитие или грешка
- Замесени клиенти и отговорен персонал

7.6. Запазване на лог-файловете /дневниците/ в Rapid7

„Бони Холдинг“ съхранява лог-файловете /дневниците/, съдържащи записи за потребителска активност, изключения и нарушения на сигурността в системата Rapid7, за минимум дванадесет (12) месеца. Тези лог-файлове /дневници/ служат като доказателство за разследвания и наблюдение на контрола на достъпа.

7.7. Съдържание на лог-файловете /дневниците/

Контролните записи включват:

- Уникални потребителски имена или идентификатори
- Дата, час и подробности за ключови събития (напр. стартиране/изключване на системата)
- Идентификация на крайно устройство или местоположение, където е възможно
- Записи на успешни и отказани опити за достъп
- Записи на успешни и отказани опити за достъп до данни/ресурси
- Промени в системната конфигурация
- Използване на привилегировани акаунти
- Мрежови адреси и протоколи
- Активиране/деактивиране на модули за сигурност
- Неоторизирани изтегляния или споделяне на съдържание

7.8. Съхранение и управление на лог-файловете /дневниците/

Всички събития се съхраняват в защитени хранилища. „Бони Холдинг“ делегира управлението, контрола на съдържанието и анализа на тези лог-файлове /дневници/ на външен Оперативен център за защита (SoC). Вътрешните специалисти нямат право да изтриват, деактивират или променят записи в логовете.

7.9. Мониторинг на областите на фокус

Мониторингът акцентира върху:

- Оторизиран достъп: Потребителски идентификатори, времеви отпечатащи, типове събития, файлове, до които е осъществен достъп, и използвани инструменти
- Привилегировани операции: Използване на администраторски, специализирани или операторски акаунти; стартиране/рестартиране/изключване на системата
- Неоторизиран достъп: Неуспешни действия, нарушения на правилата, предупреждения за защитна стена и предупреждения за откриване на проникване
- Промени в конфигурацията за сигурност: Опити за промяна на настройките или контролите за сигурност

7.10. Защита на лог-файловете /дневниците/

Въведени са механизми за защита на лог-файловете /дневниците/ от неоторизирано разкриване, промяна или изтриване. Ключовите защити включват:

- Ограничен достъп до лог-файловете /дневниците/
- Прегледът на лог-файловете /дневниците/ се извършва от квалифициран специалист от външния Оперативен център за защита (SoC)
- „Бони Холдинг“ счита информацията, записана в централизиран локални/облачни системи, за достатъчна. Лог-файловете /дневниците/ файлове включват:
 - Времеви отпечатък на успешни или неуспешни събития
 - Подробности за събитие или грешка
 - Замесени акаунти и отговорен персонал

7.11. Мониторинг на системната и потребителската активност

Дружество „Бони Холдинг“ е внедрило механизми за наблюдение на потребителската и системната активност, включително:

- Входящ/изходящ мрежов, системен и приложен трафик
- Достъп до системи, сървъри, мрежово оборудване, системи за наблюдение и критични приложения
- Конфигурационни файлове на критично или административно ниво
- Логове от инструменти за сигурност (антивирус, IDS, IPS, уеб филтри, защитни стени)
- Дневници на събития, свързани със системната и мрежовата активност

- Използване на ресурси (процесор, диск, памет, трафик) и производителност
- Установена е базова линия за сигурност за нормално поведение; отклоненията се наблюдават
- Модели на употреба по време на нормални и пикови периоди
- Типични времена за достъп, местоположения и честота на потребител/група
- Поведенчески показатели като:
 - Дейност или трафик, свързани със зловреден софтуер, от известни злонамерени IP адреси/домейни
 - Известни модели на атака (напр. DoS, препълване на буфера)
 - Необичайно системно поведение (напр. инжектиране на процеси, злоупотреба с протоколи)
 - Претоварвания и изчакване на данни (напр. мрежови опашки, латентност, трептене)
 - Неоторизиран достъп или сканиране на системи, приложения или мрежи
 - Успешни/неуспешни опити за достъп до защитени ресурси (напр. DNS сървъри, уеб портали, файлови системи)
 - Необичайно поведение на потребителя/системата в сравнение с очакваните стандарти

7.12. Докладване на инциденти

Необичайните събития се регистрират като инциденти и се докладват на съответните заинтересовани страни след категоризиране и потвърждение от външната система за контрол (SoC). Процесът на мониторинг има за цел:

- Подобряване на възможностите за одит
- Подобряване на оценката на риска
- Засилване на реакцията при инциденти
- Минимизиране на въздействието на нежеланите събития
- Идентифициране и намаляване на фалшивите положителни резултати, които биха могли да прикрият реални заплахи за дейността на „Бони Холдинг“

8. Механизми за мрежов контрол

8.1. Надзор и споразумения

Ръководството редовно следи способността си да управлява вътрешните мрежови услуги и оценява способността на доставчиците на мрежови услуги сигурно да предоставят договорени услуги. Установяват се споразумения за сигурност, изисквания за ниво на обслужване, протоколи за управление и права за одит. „Бони Холдинг“ гарантира, че доставчиците прилагат договорените мерки за сигурност.

8.2. Ключови функции и технологии за мрежова сигурност

- Интернет свързаност - Управляваните устройства за маршрутизиране се използват за осигуряване на сигурен интернет достъп в цялата организация.
- Виртуални частни мрежи (VPN) - „Бони Холдинг“ използва VPN технология, за да изгради сигурни тунели между своята инфраструктура и тази на клиенти, доставчици и служители. Тези тунели се реализират с помощта на SSL VPN или IPSec, осигурявайки удостоверяване и сигурно предаване на данни през ненадеждни мрежи.
 - IPSec протоколът се използва за удостоверяване и криптиране.
 - Отдалеченият достъп се инициира чрез VPN клиент, който се свързва с мрежово устройство (например рутер или защитна стена).
 - Удостоверяването включва уникално потребителско име, парола и сертификат, които се проверяват при всеки опит за свързване.
 - Успешното удостоверяване позволява на отдалечени потребители да имат достъп до ресурси в локалната мрежа на „Бони Холдинг“.
 - Обменът на данни с трети страни може да се осъществява чрез SSL VPN или IPSec тунели.
- Маршрутизиране - Статичните маршрути са конфигурирани за управлявани мрежови класове и подмрежи, където е приложимо.
- Преобразуване на мрежови адреси (NAT) - „Бони Холдинг“ използва NAT, за да скрие идентичността на вътрешните ресурси. Имплементацията следва RFC1918, което позволява използването на всички частни IP адреси, дефинирани в стандарта.
- Защита на имейла - Имейл комуникациите са защитени с помощта на TLS 1.3 криптиране в Microsoft 365.

9. Сигурност на мрежовите услуги

9.1. Надзор и споразумения

Ръководството редовно следи способността си да управлява вътрешните мрежови услуги и оценява способността на доставчиците на мрежови услуги сигурно да предоставят договорени услуги. Установяват се споразумения за сигурност, дефиниции на нивата на обслужване, изисквания за управление и права за одит. „Бони Холдинг“ гарантира, че доставчиците прилагат договорените мерки за сигурност.

9.2. Ключови характеристики и параметри за сигурност на мрежовите технологии

- Интернет свързаност - „Бони Холдинг“ използва Sophos XGS Firewall устройства с всички съответни абонаменти за управление на интернет свързаността в цялата организация.

- Безжични комуникации – Безжичните мрежи са базирани на стандартите IEEE 802.11n/ac/ax, работещи на честотни ленти 2.4 GHz или 5 GHz. Криптирането се осигурява чрез WPA2 с AES 256-bit. Служителите, работещи дистанционно, са инструктирани да използват същите защитени протоколи за криптиране за безжични връзки.
- Виртуални частни мрежи (VPN) – VPN мрежите се използват за установяване на защитени тунели между инфраструктурата на „Бони Холдинг“ и нейните клиенти или служители.
 - Реализирано с помощта на SSL VPN и IPSec протоколи
 - Осигурява удостоверяване и сигурно предаване на данни през ненадеждни мрежи
 - Отдалеченият достъп се инициира чрез VPN клиент, свързващ се със защитна стена
 - Удостоверяването включва уникално потребителско име, парола и сертификат
 - Успешното удостоверяване предоставя достъп до вътрешни мрежови ресурси
 - Обменът на данни с трети страни се поддържа чрез SSL VPN или IPSec тунели
- Преобразуване на мрежови адреси (NAT) – NAT се използва за скриване на вътрешните идентичности на ресурсите. Имплементацията е в съответствие с RFC1918, което позволява използването на всички частни IP адреси, дефинирани в стандарта.
- Защита на имейла – Имейл комуникациите са криптирани с помощта на TLS 1.3 в Microsoft 365.

10. Филтриране на уеб съдържание

10.1. Филтриране на трафика

Трафикът между системите и техните подсистеми се контролира чрез подходящи механизми за филтриране (напр. по IP адрес, протокол, номер на порт от TCP/IP стека и др.).

10.2. Филтриране на потребителския трафик

Задължителните указания за филтриране включват:

- Блокиране на достъпа до уебсайтове с лоша репутация чрез NGFW (защитна стена от следващо поколение) и/или софтуер за защита на крайни точки, инсталиран на потребителските устройства
- Ограничаване на уеб трафика от геолокации, които не са типични за дейността на „Бони Холдинг“

- Мониторинг, анализ и блокиране на командно-контролни (C2) сървъри, свързани със злонамерена дейност
- Блокиране на достъпа до уебсайтове с незаконно съдържание, като например торент тракери и сайтове, разпространяващи нелицензиран софтуер

10.3. Управление на портове и наблюдение на периметъра

Ненужните TCP и UDP портове се деактивират чрез правилна конфигурация на софтуерни решения, хардуерни устройства и оборудване за контрол на трафика. IP периметърът на компанията се наблюдава непрекъснато с помощта на специализирани инструменти (напр. Shodan), за да се предупреждават заинтересованите страни за новооткрити или модифицирани услуги/портове.

11. Управление на промените

11.1. Общи принципи

Всички промени, свързани със съоръженията и системите за обработка на информация, се документират и управляват. „Бони Холдинг“ се стреми да предотвратява неоторизирани промени, за да минимизира рисковете за сигурността. Отговорностите за управление на промените са ясно определени и са въведени механизми за осигуряване на ефективен контрол върху значителните промени в инфраструктурата, хардуера, комуникационните системи, операционните системи, софтуерните приложения, бизнес процесите, процедурите и технологиите.

11.2. Процес на управление на промените

Процесът включва:

- Заявки за промени: Инициират се от служители или клиенти чрез системата за заявки (support.baselineit.eu) или по имейл до ръководството. Заявките се преглеждат от мениджъра, който решава за одобрение, срокове и изпълнение.
- Тригери за промяна (без да се ограничават само до):
 - Внедряване или преконфигуриране на критичен хардуер
 - Внедряване или надграждане на операционни системи
 - Внедряване или надграждане на бизнес приложения
 - Промени в установените процедури
- Възлагане: Промените се възлагат от Управителя на квалифицирани специалисти или трети страни по договор.
- Надзор на изпълнението: Мениджърът контролира изпълнението.
- Документация: Одобрените промени се записват в специална база данни с контролиран и проследим достъп.

- Записите за промени включват:
 - Описание на промяната
 - Планирано действие
 - Очаквани и реални резултати
 - Статус на одобрение
 - Приемане или отхвърляне на новото състояние
 - Опции за връщане към стабилно предишно състояние
- Системна документация: Актуализациите могат да бъдат отразени в свързани документи, диаграми, процедури и системи.
- Уведомяване: След успешно внедряване, отговорният персонал трябва да уведоми съответните заинтересовани страни.
- Оперативни промени: Инициират се само когато е оправдано, като например въвеждане на нова функционалност или справяне с повишен риск.

12. Контрол на достъпа и управление на самоличността

12.1. Принципи на контрола на достъпа

Контролът на достъпа е критичен компонент от рамката за сигурност на „Бони Холдинг“ и се основава на принципите „необходимост да се знае“ и „минимални привилегии“. Механизмите за идентификация се управляват централизирано от външни партньори, за да се гарантира проследимост и контрол.

12.2. Централизирано управление на самоличността

- Потребителските акаунти се управляват чрез Active Directory (локално) и Microsoft 365 (облак), администрирани от външен ИТ партньор.
- Достъпът до облачните услуги се контролира чрез Azure Active Directory, синхронизиран с локалната директория.

12.3. Идентификация и удостоверяване

- На всеки потребител се предоставя уникално потребителско име и персонализирана парола.
- Многофакторното удостоверяване (MFA) е задължително за:
 - Microsoft 365
 - VPN връзки и отдалечен достъп
- Административните акаунти са отделени от стандартните потребителски акаунти и са защитени с допълнителни мерки за сигурност.

12.4. Управление на пароли – Изисквания

- Минимум 12 символа
- Трябва да включва букви, цифри и специални символи
- Паролите трябва да се сменят на всеки 90 дни
- Повторното използване на последните 5 пароли е забранено

12.5. Унифицирана политика за пароли

Политиката за пароли се прилага еднакво за всички системи, включително ERP, Active Directory, локални сървъри и облачни услуги.

12.6. Контрол на достъпа, базиран на роли (RBAC)

- Членството в групи в Active Directory определя нивата на достъп до ресурси.
- Разрешенията се предоставят въз основа на длъжностните роли (напр. Оператор, Счетоводител, Мениджър на обект, ИТ администратор).
- Достъпът до критични системи (ERP, файлови сървъри, SIEM) е ограничен само до оторизиран персонал.

12.7. Управление на достъпа за външни доставчици

- Външните ИТ доставчици и Оперативният център за защита (SoC) имат строго ограничен административен достъп, регулиран от договора и политиката за сигурност.
- Достъпът е ограничен във времето и се наблюдава в реално време чрез SIEM системата.

13. Управление и докладване на инциденти

13.1. Стратегически подход

„Бони Холдинг“ счита управлението на инциденти за ключов компонент от своята рамка за информационна сигурност. Целта е да се осигури своевременно откриване, ескалация, анализ, реагиране и възстановяване от събития, които заплашват:

- Информационни активи
- Непрекъснатост на бизнеса
- Поверителност на данните

В съответствие с Директивата NIS2 и националните регулаторни изисквания е създаден План за реагиране при инциденти (IRP).

13.2. Определение за инцидент със сигурността

Инцидент със сигурността се определя като всяко събитие, което:

- Компрометираща или има потенциал да компрометираща:
 - Поверителността
 - Почтеността
 - Наличността на системи, данни или услуги
- Прекъсва производството или ИТ процесите
- Води до:
 - Неоторизиран достъп
 - Злоупотреба с привилегии
 - Нарушения на данни
 - Измама
 - Изтичане на данни

13.3. Роли и отговорности

- партньор от Оперативния център за защита (SoC) – 24/7 наблюдение, предупреждения, първоначален анализ и действия за реагиране от първо ниво
- ИТ партньор – Техническа поддръжка, блокиране на достъп, възстановяване и проверка на лог-файлове /дневниците/
- Главен изпълнителен директор – Одобрение за уведомяване на Министерството на електронното управление (МЕУ), вземане на стратегически решения
- Контактното лице на МЕУ – Уведомяване в рамките на 24 часа след установяване на сериозен инцидент

13.4. Процес на управление на инциденти

- Откриване – чрез SIEM (Rapid7 InsightIDR) или доклади от персонал/доставчици на услуги
- Оценка – Оперативният център за защита (SoC) анализира обхвата, въздействието и сериозността
- Ескалация – уведомен е Главният изпълнителен директор
- Реакция – засегнатите услуги се спират, достъпът се блокира и засегнатите страни се информират
- Възстановяване – възстановяване от резервни копия /бекъп/ (Veeam), почистване на засегнати активи

- Документация – доклад за инцидент, извлечени поуки и последващи действия

13.5. Уведомяване на надзорния орган

- За инциденти, класифицирани като значителни, „Бони Холдинг“ трябва да уведоми Министерството на електронното управление (МЕУ) в рамките на 24 часа от откриването им.
- Докладът трябва да включва:
 - Естество на инцидента
 - Засегнати активи
 - Време за откриване и реакция
 - Предприети действия
 - Потенциални последици
- В рамките на 72 часа, „Бони Холдинг“, с подкрепата на своите партньори, трябва да идентифицира всички засегнати страни и да предостави тази информация на МЕУ, съгласно процедурите си.
- В рамките на 30 дни, „Бони Холдинг“ трябва да представи окончателен доклад на МЕУ, включително заключенията и цифровите артефакти, открити по време на разследването. Ако не се изискват допълнителни действия, инцидентът се счита за разрешен.

14. Роли и отговорности

- **Главен изпълнителен директор (ГИД)**
 - Одобрява политиката за информационна сигурност и свързаните с нея планове
 - Взема стратегически решения в случай на големи инциденти или нарушения
 - Разпределя бюджета и определя приоритетите за сигурност
 - Одобрява планове за обучение и финансира инициативи за обучение
- **Доставчик на външен Оперативен център за защита (SoC)**
 - Осигурява 24/7 системен мониторинг чрез Rapid7 InsightIDR
 - Анализира инциденти, реагира и издава известия
 - Управлява уязвимостите, използвайки InsightVM
 - Предлага консултации по сигурността и техническа поддръжка
- **Външни ИТ доставчици**
 - Управлят Active Directory, Microsoft 365, ERP системи и runZero
 - Инсталират, актуализират и поддържат крайните точки и сървъри
 - Поддържат мрежовата инфраструктура

- **Служители и оператори**
 - Спазват политиките и вътрешните разпоредби
 - Участват в задължително обучение
 - Докладват подозрителни инциденти или поведение

- **Експертен персонал**
 - Ще бъдат разпределени бъдещи роли, включително: CISO / DPO / вътрешен ИТ координатор за оперативен контрол и координация с външни доставчици

15. Обучение и осведоменост

15.1. Стратегическо значение

„Бони Холдинг“ осъзнава, че служителите са едновременно най-ценният актив и потенциална уязвимост в контекста на киберсигурността. Поради това организацията възприема систематичен подход към обучението и осведомеността, за да гарантира, че всички служители могат да разпознават рисковете и да реагират по подходящ начин на подозрителни ситуации.

15.2. Обща политика

Всички служители с достъп до информационни активи са длъжни да преминават годишно обучение по киберсигурност, провеждано от външен партньор или чрез платформа за електронно обучение.

Новоназначените служители трябва да завършат обучение по киберсигурност в рамките на първите 30 дни от назначаването си на работа.

15.3. Теми за обучение

- Основи на киберсигурността
- Социално инженерство и фишинг атаки
- Политики за пароли и защита на достъпа
- Безопасно боравене с имейли и документи
- Безопасно използване на устройства и интернет
- Процедури за реагиране при инциденти
- Отговорности при работа с чувствителна информация (включително лични данни)

15.4. Методи на обучение

- Онлайн платформи с тестове и оценки
- Присъствени семинари или ателиета
- Симулирани фишинг кампании
- Ролеви упражнения (тренировки) за реагиране при инциденти

15.5. Документация и съответствие

- Води се регистър на обучението, в който се записват датите, имената на участниците и резултатите от тестовете
- Ръководството и Оперативният център за защита (SoC) наблюдават спазването на изискванията и честотата на обучението
- Незавършването на обучението може да доведе до ограничен достъп до информационни активи

16. Преглед и актуализации

Политиката се преглежда и актуализира поне веднъж годишно или когато има значителни промени в законодателството, технологиите или бизнес процесите.

Служителят от Оперативния център за защита (SoC) (понастоящем представяван от външния Оперативен център за защита (SoC)) отговаря за провеждането на прегледа и отправянето на препоръки.

Политиката влиза в сила от датата на подписването ѝ и е задължителна за всички служители, партньори и доставчици на услуги, които имат достъп до информационните системи на компанията.

„Бони Холдинг“ се ангажира редовно да преразглежда Политиката за информационна сигурност, за да осигури постоянно съответствие със съответното законодателство на ЕС и национално законодателство и прилагане на най-добрите практики в областта.

17. Непрекъснато усъвършенстване

Дружество „Бони Холдинг“ е поело ангажимент да осигури устойчивост и предвидимост на своите ИТ-зависими производствени процеси и бизнес дейности. Постигането на това изисква внедряването на нови технологии, инструменти за киберсигурност, услуги и документация, съобразени с оценката на риска на организацията.

Поставили сме си следните ключови стратегически цели:

- Внедряване на ефективен и ефикасен процес за управление на киберсигурността в съответствие с *Наредбата за минималните изисквания за мрежова и информационна сигурност (MRNIS)*.
- Осигуряване на киберустойчивост чрез внедряването на внимателно подбрани инструменти и технологии за сигурност.
- Намаляване на риска от киберинциденти чрез непрекъснато наблюдение и анализ на поведението на информационните системи и потребителите.
- Постигане на готовност за откриване, докладване и реагиране на инциденти, като се минимизират потенциалните щети.
- Управляване на известни и нововъзникващи уязвимости чрез подобряване на ефективността на мерките за реагиране или въвеждане на нови.
- Ясно дефиниране и разделяне на ролите и отговорностите, свързани със сигурността и управлението на ИТ процесите в рамките на „Бони Холдинг“.
- Извършване на информирани оценки на риска, последвани от планове за разработка, насочени към постигане на измерими подобрения.
- Осигуряване на целенасочено и ефикасно използване на публични средства за подкрепа на киберсигурността и ИТ дейностите.
- Дейности, възлагани на външни доставчици, за които „Бони Холдинг“ липсва необходимата вътрешна експертиза.
- Документиране и редовно актуализиране на отговорностите, дейностите и процесите, свързани с ИТ дейностите и киберсигурността.
- Подкрепяне на бизнес целите си чрез внедряване на ефективни мерки за сигурност, които осигуряват непрекъснатостта на ИТ-зависимите процеси.
- Въвеждане на процес за управление на услугите, предоставяни от „Бони Холдинг“ на своите обучаващи се, като устойчивостта и сигурността са ключови показатели за успех.

18. Връзка с други документи

- Договорни клаузи за киберсигурност с доставчици и клиенти
- Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМци и разпоредби
- Политика за оценка на риска (извършена в пълно съответствие с НМИМИС)

Номер на версията	Одобрил	Дата на периодичен преглед	Изпълнено от	Дата на следващия преглед
1.0	Решение на Съвета на директорите от 05.06.2025 г.			01.07.2026

