ПОЛИТИКА ПО КИБЕРСИГУРНОСТ В „СЛЪНЧО“АД

Настоящата политика по киберсигурност е разработена съобразно Закона за киберсигурност (ЗКС) и ПРАВИЛА за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (Правилата).

1. ОБХВАТ И ПРИЛОЖИМОСТ

Политиката обхваща всички аспекти на дейността на „Слънчо“АД, свързани с информационната сигурност. Тя се отнася до всички служители, независимо от длъжност и ниво в йерархията. В нейния обхват попадат всички информационни системи и бази данни, използвани от дружеството, както и всички устройства, свързани с информационната инфраструктура. Политиката обхваща също външните доставчици на ИТ услуги и поддръжка, както и всички партньори, които имат достъп до информационни ресурси на дружеството.

2. ОСНОВНИ ПРИНЦИПИ И ЦЕЛИ

2.1. Принципи

Политиката по киберсигурност на „Слънчо“АД се основава на следните принципи:

1. Поверителността осигурява защита на информацията от неоторизиран достъп, гарантирайки че само упълномощени лица могат да получат достъп до чувствителни данни.
2. Целостта като принцип защитава точността и непроменяемостта на данните, предотвратявайки неоторизирани модификации.
3. Наличността гарантира, че информацията и системите са достъпни за оторизираните потребители в момента, когато имат нужда от тях, което е от съществено значение за непрекъснатостта на административните процеси.
4. Принципът на отчетност позволява проследяване на действията на всички потребители, създавайки ясна следа за отговорност.
5. Допълвайки общата рамка, принципът на неотричане гарантира, че извършените действия в системите не могат да бъдат отречени от лицата, които са ги предприели.

2.2. Цели

Политиката по киберсигурност има следните цели:

1. Защитата на информационните активи от външни и вътрешни заплахи, което включва предотвратяване на неоторизиран достъп, промяна или унищожаване на информацията.
2. Спазването на законовите и регулаторни изисквания.

3. Минимизирането на риска от инциденти, свързани с киберсигурността, цели ограничаване на потенциалните щети и разходи в случай на нарушение на сигурността.
4. Осигуряването на непрекъснатост на услугите при възникване на инциденти позволява дружеството да продължи да функционира ефективно дори при проблеми със сигурността.
5. Повишаването на осведомеността на служителите е особено важно, тъй като човешкият фактор е най-уязвимото звено в защитата на информацията.
6. Ефективното управление на взаимоотношенията с външни доставчици на ИТ услуги.

3. ОРГАНИЗАЦИОННА СТРУКТУРА И ОТГОВОРНОСТИ

3.1. Ръководство

Изпълнителния директор носи крайната отговорност за цялостното състояние на киберсигурността в дружеството . Неговата роля е от стратегическо значение, тъй като осигурява необходимите ресурси в рамките на финансовите възможности на дружеството.

3.2. Отговорно лице за мрежова и информационна сигурност

В съответствие със Закона за киберсигурност в дружеството се определя Отговорно лице за мрежова и информационна сигурност (ОЛИМС) което отговоря за мрежовата и информационната сигурност в дружеството. Това лице координира всички дейности по киберсигурността, включително разработване и актуализиране на вътрешните политики и процедури. ОЛМИС служи като основна точка за контакт с външни доставчици на ИТ услуги и отговаря за своевременното докладване на инциденти, съгласно законовите изисквания. Важна част от неговите отговорности е координирането на обученията на служителите относно киберзаплахите и добрите практики. За осигуряване на бързо вземане на решения, ОЛМИС докладва директно на Изпълнителния директор по всички въпроси, свързани с киберсигурността, без междинни нива на управление.

3.3. Външни доставчици на ИТ услуги

Тези доставчици осигуряват необходимата техническа експертиза и поддръжка, която не би могла да бъде осигурена с вътрешни ресурси. Те са отговорни за внедряването и управлението на технически мерки за сигурност, като антивирусна защита, защитни стени, системи за откриване на проникване и други. При възникване на инциденти, външни ИТ специалисти оказват съдействие за ограничаване на щетите и възстановяване на нормалната работа. Те също така предоставят редовни консултации и препоръки за подобряване на цялостната сигурност на информационната инфраструктура.

3.4. Отговорности на персонала на дружеството

Персонала на дружеството имат съществена роля в поддържането на ефективна система за киберсигурност. Те са длъжни да се запознаят и стриктно да спазват всички правила за киберсигурност, приложими за тяхната дейност. Отговорността на работниците/служителите включва своевременно докладване на подозрителни дейности или инциденти на ОЛМИС, като предоставят цялата налична информация, която би

помогнала за бърза реакция. Активното участие в организираните обучения по киберсигурност е задължение на всички служители, тъй като повишаването на информираността е ключов елемент от общата защита. В ежедневната си работа, персонала трябва да използват информационните системи отговорно и в съответствие с установените изисквания, като избягват рисково поведение, което би могло да застраши сигурността на дружествените информационни активи.

4. УПРАВЛЕНИЕ НА РИСКА

4.1. Базова оценка на риска

Управлението на риска започва с процес на оценка на риска. Дружеството, с помощта на свои експерти или външния ИТ доставчик, извършва оценка на риска веднъж годишно, за да идентифицира основните заплахи и уязвимости. Първата стъпка е идентифицирането на най-критичните информационни активи – системи, данни и процеси, чието компрометиране би имало сериозно въздействие върху дейността на дружеството. След определяне на критичните активи, се извършва анализ на основните заплахи, специфични задружеството, като например фишинг атаки, зловреден софтуер и социално инженерство. Оценката включва и анализ на потенциалното въздействие върху административните услуги в случай на успешна реализация на заплахите, като се фокусира върху най-вероятните сценарии.

4.2. Третиране на риска

След идентифициране и оценка на рисковете, дружеството предприема конкретни действия за тяхното третиране. Мерките за защита се избират така, че да съответстват на наличните ресурси и капацитет на дружеството. Фокусът се поставя върху най-критичните заплахи, които представляват най-голям риск, като се прилага принципът "максимална защита с минимални ресурси". Всички внедрени мерки подлежат на периодично преразглеждане, за да се гарантира тяхната продължаваща ефективност в променящата се среда на заплахи.

5. БАЗОВО УПРАВЛЕНИЕ НА ДОСТЪПА

5.1. Управление на потребителските акаунти

Ефективното управление на потребителските акаунти е основополагащ елемент от цялостната стратегия за киберсигурност. В основата на този процес стои принципът на "минимални привилегии", при който всеки потребител получава само тези права за достъп, които са абсолютно необходими за изпълнение на служебните му задължения. Това значително ограничава потенциалните щети в случай на компрометиране на акаунт. От особена важност е своевременното премахване на потребителските акаунти при напускане на работници/служители, което предотвратява възможността за неоторизиран достъп чрез стари, неактивни акаунти. За предотвратяване на натрупването на излишни права с течение на времето, дружеството провежда годишен преглед на правата за достъп. При този преглед се проверява дали съществуващите права съответстват на текущите длъжности и отговорности на служителите, като неизползваните или ненужни права се премахват.

5.2. Автентикация

Надеждната автентикация на потребителите е критичен компонент за защита на информационните системи. Дружеството изисква използването на сложни пароли, които включват минимален брой символи. За защита от неоторизиран достъп до незащитени работни станции, всички системи са конфигурирани да извършват автоматично заключване на потребителските сесии след период на неактивност. За отключване отново се изисква пълна автентикация, което осигурява допълнително ниво на защита.

5.3. Контрол на достъпа до мрежата

Контролът на достъпа до мрежата включва няколко ключови мерки, внедрени с помощта на експерти от дружеството или външния ИТ доставчик. Базовото сегментиране на мрежата разделя различните типове системи и данни, ограничавайки възможностите за неоторизиран достъп между сегментите. За служителите, които се нуждаят от отдалечен достъп до ресурсите на дружеството, се осигуряват защитени връзки чрез виртуални частни мрежи (VPN) с криптиране на комуникацията и строга автентикация. Това е особено важно в контекста на нарастващата тенденция за дистанционна работа. Допълнителна мярка е ограничаването на достъпа на посетители до отделна гостуваща мрежа, която е изолирана от вътрешната мрежа на дружеството, предотвратявайки потенциални рискове от външни устройства.

6. ОСНОВНИ МЕРКИ ЗА ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР

6.1. Антивирусна защита

Защитата от вредоносен софтуер е една от най-важните мерки за киберсигурност в дружеството. Основата на тази защита е инсталирането и поддържането на актуален антивирусен софтуер на абсолютно всички устройства, свързани към информационната инфраструктура – сървъри, работни станции, лаптопи и мобилни устройства. За максимална ефективност, антивирусните решения са конфигурирани да извършват автоматично актуализиране на дефинициите веднага след публикуването им от производителя. Това гарантира защита срещу новооткрити заплахи без необходимост от ръчна намеса. Допълнителна мярка е периодичното сканиране на всички системи за наличие на зловреден код, което позволява откриване на потенциални заплахи, които може да са били пропуснати при първоначалната проверка.

6.2. Защита от зловреден код

Освен традиционните антивирусни решения, дружеството забранява инсталирането на неоторизиран софтуер на работните станции и сървърите. Това предотвратява въвеждането на потенциално опасни програми в мрежата и намалява повърхността за атака. За допълнително ограничаване на риска, потребителите нямат административни права на своите работни станции, което възпрепятства инсталирането на софтуер без подходящо одобрение. Специално внимание се отделя на защитата на електронната поща от фишинг атаки, тъй като това е един от най-често използваните вектори за доставяне на зловреден код. Филтрирането на електронната поща блокира съобщения със съмнително съдържание преди те да достигнат до потребителите.

7. УПРАВЛЕНИЕ НА АКТУАЛИЗАЦИИТЕ

Своевременното инсталиране на актуализации за операционните системи и приложенията е критично за отстраняване на известни уязвимости, които могат да бъдат използвани от злонамерени лица. За улесняване на този процес и намаляване на административната тежест, системите са конфигурирани за автоматично изтегляне и инсталиране на актуализации, където това е технически възможно и безопасно. Този подход гарантира, че защитата се поддържа актуална без необходимост от постоянна ръчна намеса. За системи, при които автоматичното актуализиране не е препоръчително поради специфични изисквания или риск от несъвместимост, собствените експерти или външният ИТ доставчик извършват месечна проверка за налични актуализации и ги прилага контролирано след тестване в непродуктивна среда.

8. БАЗОВА СИГУРНОСТ НА КОМУНИКАЦИИТЕ

8.1. Мрежова сигурност

Защитата на комуникационните канали в мрежовата инфраструктура на дружеството е от ключово значение за осигуряване на поверителността и интегритета на предаваната информация. Основен елемент в тази стратегия е използването на актуални криптографски протоколи за криптиране на чувствителни данни, които се предават през мрежата. Комуникационните канали, особено тези, които преминават през публични мрежи, са защитени със силно криптиране, използвайки съвременни версии на протоколите. Особено внимание се отделя на безжичните мрежи, които поради своя характер са потенциално по-уязвими. За тяхната защита се прилага съвременни протоколи с цел осигуряване на значително по-високо ниво на сигурност в сравнение с предходните версии. За откриване на потенциални проблеми или аномалии, експерти от дружеството или външният ИТ доставчик извършват периодичен преглед на журналните файлове от мрежовите устройства, търсейки модели, които могат да индикират опити за неоторизиран достъп.

8.2. Електронна поща

Електронната поща като основен комуникационен канал изисква специално внимание поради високата експозиция към външни заплахи. Дружеството внедрява система за филтриране на електронната поща, която ефективно защитава от спам и фишинг съобщения, предотвратявайки достигането на потенциално опасни съобщения до крайните потребители. Всички прикачени файлове, получени по електронната поща, автоматично се сканират за зловреден код преди да бъдат доставени до пощенските кутии на работниците/служителите. Това позволява откриване и блокиране на скрити заплахи, преди те да причинят щети. Допълнителна мярка е блокирането на известни опасни типове файлове, като например изпълними файлове (.exe, .bat, .cmd), които често се използват за разпространение на зловреден софтуер. Тези файлове се задържат от системата и се освобождават само след допълнителна проверка от ИТ специалист.

9. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

9.1. Базови процедури за управление на инциденти

Ефективното управление на инциденти със сигурността е критично за минимизиране на негативното въздействие върху операциите на дружеството. В основата на този процес стои определянето на ясни стъпки за реакция при възникване на различни типове

инциденти. Дружеството разработва и документира опростени, но ефективни процедури, които описват необходимите действия при различни сценарии – от загуба на данни и заразяване със зловреден софтуер до физически нарушения на сигурността. За улесняване на координацията при инциденти, се създава и поддържа актуален списък с контакти на всички отговорни лица и експерти, които трябва да бъдат уведомени в зависимост от естеството и сериозността на инцидента. За справяне с по-сложни инциденти, които надхвърлят вътрешния капацитет, дружеството разчита на подкрепата на външния ИТ доставчик, който предоставя специализирана експертиза и ресурси за бързо ограничаване и отстраняване на последствията (**Приложение №1**).

9.2. Докладване на инциденти

Своевременното и точно докладване на инциденти със сигурността е от ключово значение за ефективната реакция в следните срокове:

- Значителен инцидент – ранно уведомяване: до 24 часа от узнаването
- Подробно уведомление: до 72 часа от узнаването
- Окончателен доклад – не по-късно от един месец след уведомлението, а при продължаващ инцидент – до един месец след неговото овладяване

Дружеството е създало ясна верига за докладване, при която всички служители незабавно уведомяват ОЛМИС при забелязване на потенциални проблеми или инциденти. ОЛМИС оценява ситуацията и уведомява външния ИТ доставчик за техническа подкрепа, както и Изпълнителния директор при по-сериозни инциденти. В изпълнение на законовите изисквания, ОЛМИС отговаря за докладването на значимите инциденти към националните компетентни органи, включително МЕУ и националния CERT екип, спазвайки сроковете и форматите, определени в Закона за киберсигурност.(**Приложение №2** към настоящия документ)

9.3. Анализ и извличане на поуки

След приключване на инцидент, дружеството извършва опростен, но систематичен анализ на случилото се, за да идентифицира първопричините и да извлече ценни поуки за бъдещето. Този анализ включва преглед на хронологията на инцидента, предприетите действия и тяхната ефективност. На база на извлечените поуки, се актуализират мерките за защита, за да се предотврати повторното възникване на подобни инциденти. Това може да включва промени в техническите контроли, актуализиране на процедурите или допълнително обучение на служителите.

10. БАЗОВА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА

10.1. План за непрекъснатост

Осигуряването на непрекъснатост на дейността при инциденти със сигурността или други извънредни ситуации е от критично значение за функционирането на дружеството.

10.2. Създаване на резервни копия

Надеждната система за създаване на резервни копия е фундаментален елемент от стратегията за непрекъснатост на дейността. Дружеството внедрява система за

ежедневно автоматизирано създаване на резервни копия на всички критични данни, като графикът и обхватът на архивирането се определят според важността на информацията. Автоматизацията на процеса елиминира риска от пропуски поради човешка грешка и гарантира регулярност на архивирането. От изключителна важност за надеждността на процеса на възстановяване е периодичното тестване на процедурите за възстановяване от резервните копия. За осигуряване на максимална защита, резервните копия се съхраняват не само локално, но и на отдалечено местоположение или в защитено облачно хранилище, което гарантира, че дори при физическо бедствие в основната локация, данните ще останат достъпни.

11. УПРАВЛЕНИЕ НА ВЗАИМООТНОШЕНИЯТА С ВЪНШНИ ИТ ДОСТАВЧИЦИ

11.1. Изисквания към външните ИТ доставчици

Всички договори с доставчици включват конкретни клаузи за сигурност, които детайлно описват изискванията за защита на информацията, процедурите за докладване на инциденти и последствията при нарушаване на тези изисквания. Тези клаузи са правно обвързващи и гарантират, че доставчиците са задължени да спазват същото ниво на защита, което се изисква от дружеството. От особена важност е изискването за стриктно спазване на националното законодателство в областта на киберсигурността и защитата на личните данни, включително Закона за киберсигурност и Общия регламент за защита на данните (GDPR). Договорите също така определят ясни процедури за докладване на инциденти, които осигуряват своевременно уведомяване на дружеството при установяване на потенциални проблеми или нарушения на сигурността.

11.2. Мониторинг на доставчиците

Непрекъснатият мониторинг на дейностите на външните ИТ доставчици е от ключово значение за своевременно идентифициране и адресиране на потенциални рискове. На тримесечие се провеждат срещи между представители на дружеството и доставчика за обсъждане на по-стратегически въпроси, свързани със сигурността, преглед на потенциални инциденти и планиране на бъдещи подобрения. За целта служителите на външните ИТ доставчици подписват Декларация за конфиденциалност (**Приложение №4**).

12. ОБУЧЕНИЯ И ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА

12.1. Програма за базово обучение

Човешкият фактор играе ключова роля в цялостната стратегия за киберсигурност, поради което дружеството инвестира в ефективна програма за обучение на работниците/служителите. За всички новопостъпили работници/служители се провежда задължително въвеждащо обучение, което обхваща основните принципи на киберсигурността, специфичните политики на дружеството и личните отговорности за поддържане на сигурността на информационните активи (**Приложение №1 и Приложение №3**).

12.2. Повишаване на осведомеността

Освен формалните обучения, дружеството провежда непрекъснати дейности за повишаване на осведомеността на работниците/служителите относно киберзаплахите и важността на сигурното поведение. Редовното разпространение на информация за актуални заплахи помага на работниците/служителите да бъдат бдителни и да разпознават потенциалните рискове в ежедневната си работа. Тази информация се споделя чрез вътрешни канали за комуникация, като електронна поща, информационни бюлетини или кратки съобщения на информационните табла. Периодичните напомняния за добри практики в областта на киберсигурността поддържат високо ниво на внимание и предотвратяват формирането на рисково поведение поради рутина или комфорт.

13. ОСНОВНИ МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

13.1. Физически контрол на достъпа

Физическата сигурност е неразделна част от цялостната стратегия за киберсигурност, тъй като неоторизираният физически достъп до информационните системи може да компрометира и най-добре защитената мрежа. Дружеството прилага базови, но ефективни мерки за ограничаване на физическия достъп до критичните информационни системи и инфраструктура. Сървърните помещения и комуникационните шкафове са разположени в зони с ограничен достъп, като вратите са оборудвани с механични или електронни ключалки. Достъпът до тези зони е разрешен само на оторизирани лица, чиито служебни задължения изискват пряк достъп до оборудването. За контрол на достъпа се използват традиционни методи като ключове, карти за достъп или кодове, в зависимост от наличните ресурси и нивото на сигурност, което е необходимо. За посетители и външни изпълнители, които имат нужда от временен достъп до защитените зони, се прилагат специални процедури, включващи постоянно придружаване от оторизиран служител и водене на регистър на посетителите, съдържащ информация за целта на посещението и времето на влизане и излизане.

13.2. Защита на оборудването

Защитата на физическото оборудване от различни заплахи е от ключово значение за осигуряване на непрекъсната работа на информационните системи. За защита от прекъсване на електрозахранването, критичното оборудване като сървъри и комуникационни устройства е свързано към непрекъсваеми захранващи източници (UPS), които осигуряват достатъчно време за безопасно изключване на системите при продължително прекъсване на захранването. За предотвратяване на повреди поради прегряване, помещението, в което се намира сървърът е оборудвано с климатик, който поддържа подходяща температура. С цел защита от пожари, помещението е оборудвано с пожарогасител, като в рамките на бъдещи мерки е планирано монтирането на датчик за пожарно известяване.

14. БАЗОВО СЪОТВЕТСТВИЕ И ОДИТ

14.1. Спазване на законовите изисквания

Стриктното спазване на приложимото законодателство в областта на киберсигурността е основен приоритет и отговорност на дружеството. За постигане на това съответствие, дружеството провежда годишен преглед на приложимите изисквания и внедрените мерки за защита. Този преглед позволява идентифициране на потенциални пропуски и

планиране на необходимите подобрения. ОЛМИС отговаря за документирането на предприетите мерки, която служи не само за доказване на съответствие при евентуални проверки от регулаторните органи, но и като основа за непрекъснато подобрение.

14.2. Вътрешни проверки

Вътрешните проверки са важен механизъм за гарантиране на ефективното прилагане на политиките за киберсигурност. Тази самооценка се координира от ОЛМИС и включва преглед на въведените контроли, както и оценка на тяхната ефективност. Конкретни аспекти на проверката включват анализ на журналните файлове за неоторизиран достъп или други подозрителни дейности. Този анализ може да разкрие опити за пробив или други проблеми със сигурността, които може да са останали незабелязани при ежедневното наблюдение. Допълнителен елемент е тестването на основните контроли за сигурност, като например проверка на ефективността на политиките за пароли, функционирането на контрола на достъпа или способността за възстановяване на данни от резервни копия.

14.3. Периодичен външен преглед

Външният преглед предоставя независима оценка на нивото на киберсигурност в дружеството и съответствието с приложимите стандарти и регулации. Обхватът на този преглед се фокусира върху критичните системи и процеси, като се избягва излишно детайлизиране на по-малко значими области. Това позволява ефективно използване на ограничените ресурси за получаване на максимална стойност от външната експертиза. Препоръките от външния преглед се приоритизират според тяхната значимост и наличните ресурси, като се разработва реалистичен план за внедряване на най-важните подобрения. Този подход осигурява постепенно и устойчиво повишаване на нивото на сигурност, без да създава непосилна финансова или административна тежест за дружеството.

15. ПОДДЪРЖАНЕ НА АКТУАЛНА ПОЛИТИКА

15.1. Годишен преглед

Поддържането на актуална и ефективна политика по киберсигурност изисква систематичен процес на периодичен преглед и актуализация. Дружеството извършва цялостен преглед на политиката по киберсигурност веднъж годишно, за да гарантира нейната адекватност спрямо променящата се среда на заплахи, технологичното развитие и актуалните нормативни изисквания. Този преглед се координира от ОЛМИС, но включва принос от всички участници в процеса, включително представители на основните звена на дружеството и външния ИТ доставчик. Ключов аспект на прегледа е оценката на ефективността на прилаганите мерки за сигурност, която се базира на анализ на възникналите инциденти, резултатите от проверките и обратната връзка от служителите. Особено внимание се отделя на новите и нововъзникващите заплахи, които може да не са били адекватно адресирани в съществуващата политика. За тази цел, ОЛМИС следи информацията за тенденциите в киберзаплахите от публично достъпни източници и участва в информационни сесии, организирани от националните компетентни органи.

15.2. Управление на промените

Управлението на промените в политиката по киберсигурност е структуриран процес, който гарантира, че всички изменения са документирани, валидирани и ефективно комуникирани. Всяка предложена промяна, независимо дали е резултат от периодичния преглед, установен инцидент или промяна в нормативните изисквания, се документира с ясно описание и обосновка. Предложенията за промени се одобряват от Изпълнителния директор, който носи крайната отговорност за киберсигурността. След одобрение, промените се внедряват според предварително определен график, който позволява адекватна подготовка и минимизира потенциалното въздействие върху оперативните дейности. От особена важност е ефективното информиране на всички служители за промените в политиката. Това се осъществява чрез различни канали за комуникация, включително електронна поща, вътрешни съобщения или работни срещи, в зависимост от естеството и обхвата на промените.

16.Влизане в сила и актуализация

Политиката влизат в сила от датата на приемането и. Преглежда се най-малко веднъж годишно и при съществени промени в рисковете, технологиите или правните изисквания. В 10-дневен срок се създава и започва водене на Регистър на инцидентите.

ПРИЛОЖЕНИЯ

Приложение № 1: Процедура за докладване на инциденти

Приложение № 2: Формуляр за докладване на инцидент

Приложение № 3: Програма за въвеждащо обучение за новоназначени работници/ служители

Приложение № 4: Декларация за конфиденциалност

08.04.2026г.

.....

Изпълнителен директор на „Слънчо“АД
Д.Александрова

Приложение № 1

Процедура за докладване на инциденти

1. Цел

Настоящата процедура определя стъпките, които трябва да бъдат следвани при установяване, докладване и управление на инциденти, свързани с киберсигурността.

2. Обхват

Процедурата се прилага при всички инциденти, които могат да повлияят на поверителността, цялостността или наличността на информационните активи на „Слънчо“АД.

3. Отговорности

- **Всички** работниците/служителите са отговорни за докладване на подозрителни дейности или инциденти.
- **ОЛИМС** отговаря за оценка, класификация и управление на инцидентите.
- **Изпълнителния директор** отговаря за вземане на стратегически решения при значителни инциденти.

4. Етапи на процедурата

4.1. Установяване и докладване на инцидент

- Работник/служител, който установи или подозира инцидент със сигурността, незабавно уведомява ОЛИМС чрез определените канали за комуникация.

- Докладването трябва да съдържа:
- Име и контакти на докладващия
- Дата и час на установяване на инцидента
- Описание на инцидента
- Потенциално засегнати системи или данни
- Предприети действия (ако има такива)

4.2. Регистриране и класификация на инцидента

- ОЛИМС регистрира инцидента в система за управление на инциденти.
- Инцидентът се класифицира според:

- Тип на инцидента (напр. зловреден код, неоторизиран достъп, DDoS атака)
- Ниво на въздействие (ниско, средно, високо, критично)
- Обхват на засегнатите системи или данни

4.3. Реагиране на инцидента

- За всеки инцидент се определя отговорник, който да координира реакцията.
- Предприемат се незабавни действия за ограничаване на въздействието:

- Изолиране на засегнатите системи
- Блокиране на компрометирани акаунти
- Прекъсване на подозрителен мрежов трафик

- Събират се и се съхраняват доказателства за инцидента.

4.4. Възстановяване

- Разработва се и се изпълнява план за възстановяване.
- Проверява се целостта на данните и системите.
- Системите се връщат в експлоатация след потвърждение, че са защитени.

4.5. Докладване към външни организации

- За значителни инциденти (със средно, високо или критично въздействие) се уведомяват:
- Значителен инцидент – ранно уведомяване: до 24 часа от узнаването
- Подробно уведомление: до 72 часа от узнаването
- Окончателен доклад – не по-късно от един месец след уведомлението, а при продължаващ инцидент – до един месец след неговото овладяване

- Националният CERT
- Други засегнати организации или доставчици на услуги

- Докладването се извършва по стандартизирана форма, съгласно изискванията на Закона за киберсигурност.

4.6. Последващи действия

- Провежда се анализ на причините за инцидента.
- Извличат се поуки и се предлагат мерки за предотвратяване на подобни инциденти.
- Актуализират се политиките и процедурите за сигурност при необходимост.
- Провежда се допълнително обучение на служителите, ако е необходимо.

5. Документиране

- За всеки инцидент се поддържа пълна документация, включваща:

- Формуляр за докладване на инцидента
- Записи от предприетите действия
- Комуникация със заинтересованите страни
- Доклад от анализа на инцидента
- План за корективни действия

6. Периодичен преглед

- Процедурата за докладване на инциденти се преглежда и актуализира поне веднъж годишно или след значителни инциденти.

Приложение № 2

Формуляр за докладване на инцидент (образец)

Приложение- **Дата/час на откриване:**

- Открит от (име/длъжност/клас):
- Засегната система/устройство:
- Описание на събитието: _____
- Вероятно засягане на лични данни: ДА/НЕ (описание)
- Първоначални действия:
- Кой е уведомен: Координатор/Изпълнителен Директор/Изпълнител
- Подпис на подателя:
- Номер в Регистъра на инцидентите:

Приложение №3

Програма за въвеждащо обучение на новоназначени служители

1.1. Цел и обхват

Въвеждащото обучение има за цел да запознае новите работници/служители с основните принципи на киберсигурността, политиките и процедурите, действащи в дружеството, както и с личните им отговорности за поддържане на сигурността на информационните активи. Обучението е задължително за всички новопостъпили служители и се провежда в рамките на първите две седмици от постъпването им на работа.

1.2. Продължителност и формат

Обучението се провежда в рамките на един работен ден и включва теоретична и практическа част. Теоретичната част се представя под формата на презентация, придружена с конкретни примери и дискусии, а практическата част включва решаване на казуси и симулации на реални ситуации.

1.3. Съдържание на обучението

1.3.1. Основни принципи на киберсигурността

- **Въведение в киберсигурността**

- Какво представлява киберсигурността и защо е важна
- Основни понятия и терминология
- Типове киберзаплахи и атаки (фишинг, социално инженерство, злонамерен софтуер и др.)
- Статистика за инциденти в публичния сектор в България

- **Основни принципи на защитата на информацията**

- Поверителност, цялостност и наличност
- Отчетност и неотричане
- Управление на риска - основни концепции
- Многопластов подход към сигурността

- **Законова и регулаторна рамка**

- Основни изисквания на Закона за киберсигурност
- Наредба за минималните изисквания за мрежова и информационна сигурност
- Общ регламент за защита на данните (GDPR) - основни аспекти, свързани с киберсигурността

1.3.2. Политики по киберсигурност в „Слънчо“АД

Преглед на фирмената политика по киберсигурност

- Обхват и приложимост

- Роли и отговорности (ръководство, ОЛМИС, външни доставчици, служители)
- Процедури за докладване на инциденти

- **Управление на достъпа**

- Политика за пароли - изисквания за сложност и периодична промяна
- Правила за управление на потребителски акаунти
- Двуфакторна автентикация - какво представлява и как се използва
- Правила за отдалечен достъп до системите

- **Защита от зловреден софтуер**

- Антивирусна защита - как работи и защо е важна
- Правила за ползване на преносими носители (USB устройства и др.)
- Правила за инсталиране на софтуер

- **Сигурност на комуникациите**

- Безопасно използване на електронна поща
- Безопасно сърфиране в интернет
- Политика за използване на социални медии
- Правила за споделяне на информация по телефон и други канали

1.3.3. Лични отговорности и практически мерки (2 часа)

- **Практически мерки за ежедневна защита**

- Как да разпознаваме фишинг съобщения
- Безопасно съхранение и управление на пароли
- Как да защитим работната станция и мобилните устройства
- Физическа сигурност на работното място (политика на "чисто бюро", заключване на екрана)

- **Докладване на инциденти**

- Как да разпознаем потенциален инцидент със сигурността
- Процедура за докладване - към кого и как
- Каква информация да предоставим при докладване на инцидент
- Практически упражнения за докладване на различни типове инциденти

- **Непрекъснатост на работата**

- Основни принципи за непрекъснатост на работата
- Индивидуални отговорности при извънредни ситуации
- Как да работим сигурно извън офиса

Приложение № 4

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ (техник на изпълнителя)

Аз, долуподписаният, служител на, декларирам, че:

1. ще пазя в тайна и няма да разгласявам лични данни и друга защитена информация, до която получавам достъп при поддръжка на системите на „Слънчо“АД-Свищов;
2. ще използвам информацията единствено за целите на изпълнението на задачите по договора;
3. ще спазвам политиките за сигурност на Дружеството и указанията на упълномощените лица;
4. при инцидент или съмнение за инцидент ще уведомя незабавно Координатора и контактното лице по договора;
5. при прекратяване на участието ми ще върна всички носители/достъпи и ще унищожа копия.

Дата: ___/ Подпис: ___ / ЛН:/ Документ за самоличност: