ДИРЕКТИВА
май 2026

HOLCIM

ДИРЕКТИВА ЗА ПОТРЕБИТЕЛИТЕ НА ИНФОРМАЦИОННИ СИСТЕМИ

ВЪВЕДЕНИЕ И ОБХВАТ

Настоящата Директива установява правилата за приемливо използване на данни, устройства и приложения от всички ИТ потребители (както крайни потребители, така и ИТ персонал) с цел осигуряване на защита и информационна сигурност. Основната ѝ задача е да защити личните данни и да предпази Холсим от финансови и репутационни щети.

ИТ устройствата включват всички електронни устройства (напр. компютри или преносими компютри, мрежата на Холсим, принтери, сървъри, мобилни устройства), предназначени за обработка, съхранение или трансфер на електронни файлове/данни, включително предоставените от компанията ИТ устройства, лични ИТ устройства, които се използват в съответствие с политиката на Холсим за използване на собствени устройства (BYOD), или други ИТ устройства, използвани за достъп до публично достъпни уеб услуги на Холсим (напр. Google услуги на Холсим). Ако в тази Директива не е направено разграничение между служебни ИТ устройства, лични или други устройства, правилата в тази Директива се прилагат за използването на всяко едно от тях.

Обхватът на тази Директива е световен и се прилага за всички компании, контролирани от Холсим, както и за всички техни съответни служители, директори, ръководители (наричани по-долу заедно „служители на Холсим“ или „вие“) и подизпълнители. Всеки служител на Холсим е отговорен за осигуряването на съответствие с тази Директива в рамките на своята сфера на компетентност и влияние, за това да действа почтено и да спазва местните закони, Етичния кодекс на Холсим и други приложими политики и директиви на Холсим.

Холсим полага добросъвестни усилия за прилагане на тази Директива или подобни стандарти в компании, върху които няма контрол.

За да се осигури цялостно съответствие и лесно разбиране, основните принципи на тази Директива за потребителите на информационни системи са обобщени в петте задължителни правила за ИТ сигурност по-долу, които трябва да се спазват винаги. Тези правила, които трябва да бъдат подписани от всички нови служители и подизпълнители, преди да им бъде предоставен достъп до ИТ системите (шаблони за подписване от **служители** и **подизпълнители**), служат като кратко резюме на изискванията на Директивата, като подробното обяснение, примерите и специфичните задължения за всяко правило са доразвити в съответния раздел в този документ.

ПЕТ ПРАВИЛА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

ИНФОРМАЦИОННАТА СИГУРНОСТ НА МОЕТО РАБОТНО МЯСТО Е МОЯ ОТГОВОРНОСТ

ПРАВИЛО 1: ПАЗЕТЕ ПАРОЛИТЕ СИ В ТАЙНА И ЗАКЛЮЧВАЙТЕ ЕКРАНА НА КОМПЮТЪРА СИ

ПРАВИЛО 2: НЕ ИНСТАЛИРАЙТЕ НИКАКЪВ СОФТУЕР ИЛИ ХАРДУЕР НА ВАШАТА СИСТЕМА БЕЗ КОНСУЛТАЦИЯ С ИТ ОТДЕЛА

ПРАВИЛО 3: ПАЗЕТЕ ВАШИТЕ ИТ УСТРОЙСТВА И ИНФОРМАЦИОННИ АКТИВИ ОТ ПОВРЕДА ИЛИ ЗАГУБА

ПРАВИЛО 4: БЪДЕТЕ ВНИМАТЕЛНИ ОНЛАЙН. ПАЗЕТЕ СЕ ОТ РИСКОВЕ ЗА СИГУРНОСТТА ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ (AI), ИМЕЙЛ ИЛИ ИНТЕРНЕТ

ПРАВИЛО 5: ДОКЛАДВАЙТЕ ВСИЧКИ ИНЦИДЕНТИ СЪС СИГУРНОСТТА НА ИТ ОТДЕЛА

ПРАВИЛО 1: ПАЗЕТЕ ПАРОЛИТЕ СИ В ТАЙНА И ЗАКЛЮЧВАЙТЕ ЕКРАНА НА КОМПЮТЪРА СИ

Всеки потребител е длъжен да гарантира, че паролите отговарят на следните правила, дори ако ИТ системите не налагат минималните изисквания:

- Всяка парола трябва да се състои от **поне 12 знака** и да включва поне 3 от следните четири типа знаци:
  - Малки букви (a-z)
  - Главни букви (A-Z)
  - Цифри (0-9)
  - Специални знаци (напр. !, @, #, $)
- Администраторите трябва да използват пароли с **минимум 24 знака**, управлявани чрез сигурен мениджър на пароли (т.е. инструмента Passwd, който е стандартът в Холсим).
- Всяка парола трябва да се пази в тайна (напр. не я споделяйте с прекия си ръководител, асистент, ИТ отдела, ИТ администратор или друг ИТ потребител).
- Потребителските акаунти не трябва да се споделят. Вие носите отговорност за всички действия, извършени чрез вашите акаунти.
- Трябва да промените първоначално предоставените ви пароли по време на първоначалното влизане в системата.
- Трябва да използвате многофакторна автентификация (MFA) навсякъде, където е възможно (т.е. допълнително потвърждение чрез SMS код, биометрия или други видове хардуерни или софтуерни токени). Това се отнася за всички ваши корпоративни приложения.
- Когато няма въведена многофакторна автентификация, трябва периодично да сменяте паролата си, **поне на всеки 12 месеца**. Някои системи изискват смяна на всеки 3 месеца, което е направено умишлено.
- Трябва да промените паролите си за Active Directory, Google и други ключови системи в случай на съмнения за компрометиране на вашите акаунти.
- Съхраняването на пароли в хранилища е строго забранено. Паролите никога не трябва да се съхраняват в изходен код (source code), текстови файлове, електронни таблици или други незащитени места.
- Паролите не трябва да бъдат лесни за отгатване. Не използвайте думи от личната си или служебна среда (напр.: собствено/фамилно име, Холсим, села/градове, телефонни номера, рожден ден, набор от цифри, последователни пароли като „parola1“, след това „parola2“ и т.н.).
- Избягвайте повторното използване на поне последните си 5 пароли, когато бъде поискана промяна на паролата. Не използвайте механични правила за създаване, тъй като те са известни на нападателите.
- Трябва да използвате различни пароли за личния си достъп (т.е. лично ползване на интернет) и в рамките на ИТ системите на Холсим.
- Смартфоните и таблетите трябва да бъдат защитени чрез използване на потребителски пароли или ПИН код, както е описано в Правило 3, за да се предотврати достъпът на неоторизирани потребители до информация.

ПРЕДОТВРАТЯВАНЕ НА НАРУШЕНИЯ НА СИГУРНОСТТА

Следните предпазни мерки ще помогнат за намаляване на риска от нарушения на сигурността:

- Заключвайте компютъра или мобилното си устройство, когато са без надзор.
- Уверете се, че излизате (log out) от активните сесии в уеб приложенията на Холсим, особено когато използвате компютър, различен от вашия корпоративен.
- Уверете се, че чувствителни или поверителни документи не се виждат открито на бюрото ви.
- Не оставяйте преносим компютър без надзор в кола, в лобито на хотел, по време на конференция/среща или при чакане на опашка (напр. на летището).
- Поставяйте преносимите компютри, документите и служебните телефони в ръчния си багаж в самолетите.
- Винаги когато е възможно, заключвайте кабинетите и залите, в които се съхраняват компютри или други мобилни устройства.

ПРАВИЛО 2: НЕ ИНСТАЛИРАЙТЕ НИКАКЪВ СОФТУЕР ИЛИ ХАРДУЕР НА ВАШАТА СИСТЕМА БЕЗ КОНСУЛТАЦИЯ С ИТ ОТДЕЛА

СОФТУЕР

Забранено е инсталирането или модифицирането на софтуер от неоторизирани лица върху компютри и лаптопи, собственост на Холсим. Това ограничение обхваща и деинсталирането на предварително инсталиран софтуер или служебни приложения.

Всички софтуерни продукти (включително приложения, добавки (Add-ons), разширения (Extensions) и др.), използвани в Холсим, подлежат на задължителна проверка и се инсталират на корпоративните устройства единствено от съответния ИТ отдел. Инсталирането и/или използването на личен софтуер върху компютри и лаптопи, собственост на Холсим, не е разрешено, освен ако няма изрично предварително одобрение от ИТ отдела.

При инсталиране на софтуер за служебни цели от оторизиран потребител, същият е длъжен предварително да се увери, че продуктът е надлежно лицензиран и че версията му се поддържа активно от производителя. Използването на софтуер с изтекъл жизнен цикъл – „End-of-Life“ (EOL) – е строго забранено. Дори и да притежава лиценз, софтуер, който вече не се поддържа от доставчика, не може да бъде използван, тъй като за него не се осигуряват актуализации и корекции за сигурност (напр. версии на Microsoft Office, по-стари от 2021 г.).

На корпоративните устройства е разрешена употребата единствено на софтуер, официално предоставен или одобрен от ИТ отдела. Тази политика се прилага изрично и за:

- **Портативни приложения (Portable applications):** софтуер, който се изпълнява без официален процес на инсталиране (напр. торент клиенти или всякакви приложения през USB или локални папки).
- **Инсталации на потребителско ниво (User-level installations):** софтуер, който се инсталира, без да изисква администраторски права.

МОБИЛНИ УСТРОЙСТВА, СМАРТФОНИ И ТАБЛЕТИ

ИТ потребителите имат право да инсталират одобрени мобилни приложения на своите служебни устройства (смартфони и таблети). Всеки потребител носи лична отговорност за правилното използване и коректното функциониране на зачисленото му мобилно устройство.

Мобилните приложения трябва да се изтеглят единствено от официални източници, оторизирани от разработчика на съответната платформа (напр. App Store, Google Play). Инсталирането на софтуер от ненадеждни платформи е строго забранено. При колебания дали даден източник е одобрен, се свържете с ИТ отдела.

Потребителите на мобилни устройства са длъжни да осигурят следното:

- ПИН кодовете за мобилни устройства трябва да бъдат **поне 6 знака**.

- Холсим използва инструменти за управление, като например Google Mobile Device Management (MDM), за защита и подсигуряване на мобилните устройства, така че ще трябва да регистрирате устройството си, за да работи правилно. Холсим си запазва правото да откаже достъп до мобилни услуги за устройства, на които не работят правилните агенти за управление.
- Холсим има правомощието дистанционно да изтрива данни на Холсим от служебни и лични устройства (и ако е необходимо, цялото устройство), ако устройството бъде откраднато, загубено, ако трудовото правоотношение на потребителя бъде прекратено/реши да напусне организацията или при други ситуации, които могат да изискват подобни действия.
- Третирайте обществения Wi-Fi като по презумпция несигурен и незабавно прекратете връзката, ако се покажат предупреждения за сигурността от рода на „Privacy Warning“ (Предупреждение за поверителност) или „Insecure Connection“ (Несигурна връзка).
- В случай че сдвоявате устройство (напр. Bluetooth), избягвайте използването на пароли по подразбиране или отворени настройки.
- Устройствата не трябва да бъдат „разбивани“ (jailbroken) или да имат инсталиран софтуер/фърмуер, предназначен за получаване на достъп до функционалности, които не са първоначално предвидени от производителя на устройството да бъдат достъпни за потребителя. Нито пък трябва да се инсталира софтуер/фърмуер, който може да се използва за промяна или подмяна на системни приложения и настройки и изтегляне на приложения, които не са налични в официалните магазини.
- Операционната система на устройството (iOS/Android) и приложенията трябва винаги да се поддържат актуални с актуализации, предоставени от производителя или мрежата. Настройте устройството и приложенията си на автоматично актуализиране, за да сте в съответствие с тази Директива.
- Когато използват услуги за геолокация, потребителите трябва да прочетат правилата и условията, за да видят до каква информация позволяват на приложението да има достъп. Внимавайте какво споделяте. При съмнение се консултирайте с Правния отдел.
- Двуфакторната автентификация трябва да бъде активирана на всички акаунти в AppleID и iCloud, както и на подобни алтернативи на други доставчици.

Разрешено е използването само на предварително одобрени инструменти за отдалечен достъп за поддръжка и съдействие (т.е. Bomgar или Ivanti), но вие трябва да запазите контрола над връзката (т.е. да потвърдите самоличността на лицето, което се свързва, да одобрите и прекратите връзката, както и да наблюдавате всички извършвани дейности).

ЗАБРАНЕНА УПОТРЕБА

При работа със служебна информация или файлове трябва да се използват само одобрени и разрешени онлайн услуги (напр. имейл, незабавни съобщения, генеративен изкуствен интелект (Generative AI) и др.). На служителите е забранено да качват/използват каквито и да било поверителни или вътрешни работни и търговски данни или документи на Холсим, изцяло или частично, в неодобрени външни платформи или услуги.

Това включва, но не се ограничава до:

- Архивиране или споделяне на информация в услуги за облачно съхранение (напр. Dropbox, iCloud, BitTorrent); вместо това насърчаваме използването на **Google Drive** за съхранение и споделяне с трети страни.
- Услуги за съобщения (като Telegram, Signal и др.) и социални медии (напр. X, Facebook, Instagram, TikTok и др.) за споделяне на информация на Холсим. Вместо това трябва да се използват инструментите на Холсим (напр. Google Hangouts/Chat). За яснота, такива услуги за съобщения могат да се използват за вътрешни или външни комуникации, които са лични и/или не включват никакви поверителни или вътрешни работни и търговски данни или документи на Холсим. Използването на стандартен WhatsApp е строго ограничено до обща вътрешна координация и неповерителна комуникация, както при всички други услуги за съобщения, обяснени по-горе, докато използването на **WhatsApp Business** е разрешено изключително за оперативни и търговски цели, при условие че акаунтът е надлежно лицензиран и регистриран под домейна на компанията.
- Лични/частни имейл акаунти (напр. лично ползване на Hotmail, Google (Gmail), GMX Mail, Yahoo! Mail, AOL Mail и други доставчици на имейл) или всякакви други външни имейл акаунти при липса на легитимна бизнес цел.
- Платформи за сътрудничество извън корпоративните споразумения (напр. Slack, Microsoft Teams) и сайтове за съхранение на код.
- Услуги за превод (като DeepL, Amazon Translate и др.). Като безопасен метод за превод ви насърчаваме да използвате функцията **„Translate document“** (Превод на документ – когато работите с Google Docs, можете да я намерите в меню „Tools“ / Инструменти), която е вътрешен инструмент, или Google Gemini във версията, която е одобрена за бизнес употреба в Холсим.
- Сменяеми носители (флаш памети, USB устройства и др.), освен ако такива устройства не са разрешени за такава употреба от ИТ отдела. Вместо това използвайте хранилището за документи на Холсим (в момента Google Drive) за споделяне на файлове и резервно копие на данни.
- Чатботове с изкуствен интелект (AI) (някои примери включват ChatGPT, MS Bing Copilot, Jasper.ai, You.com и др.), освен ако те не са интегрирани в дигиталните решения на Холсим или по друг начин одобрени за бизнес употреба в Холсим (в момента това е така за версията на Холсим за Google Gemini и NotebookLM). Прегледайте подробностите относно използването на AI в Директивата за изкуствен интелект.

- Инструменти с AI за срещи в Zoom (напр. Otter.ai, Read.ai) не са разрешени, тъй като могат да споделят поверителни данни от срещи с трети страни. Въпреки това, инструментът **Zoom AI Companion**, който е вграден нативно, е разрешен за употреба.

Всички данни и документи трябва да бъдат класифицирани в съответствие с изискванията на Холсим за класификация на данни. Служителите трябва да направят справка с *Процедурата за класификация на информацията* за приложимите нива на класификация на данните и с *Ръководството за класификация на информацията* за насоки относно правилното боравене и управление на данни въз основа на тяхната класификация.

Правилата относно съхранението на информация могат да бъдат намерени в *Директивата за съхранение и изтриване на данни* и местните *Политики за съхранение на данни*.

ПРАВИЛО 3: ПАЗЕТЕ ВАШИТЕ ИТ УСТРОЙСТВА И ИНФОРМАЦИОННИ АКТИВИ ОТ ПОВРЕДА ИЛИ ЗАГУБА

Ако използвате вашия компютър/лаптоп за обработка на чувствителни данни на обществени места (напр. самолети), помислете за заявяване на филтър за поверителност на екрана (privacy screen filter) от ИТ отдела.

Данните не трябва да се съхраняват локално (на вашия компютър, лаптоп), вместо това те трябва да се копират в хранилището за документи на Холсим (в момента Google Drive) или на файловите сървъри на Холсим, за да се предотврати загуба на данни.

Чувствителните (поверителни/с ограничен достъп) документи на хартиен носител трябва да се заключват всяка вечер.

Белите дъски и флипчартовете трябва да се почистват от чувствителна информация, когато ги напускате (особено в залите за срещи).

ЛИЧНО ИЗПОЛЗВАНЕ НА ИТ УСТРОЙСТВА НА ХОЛСИМ И ИЗПОЛЗВАНЕ НА ЛИЧНИ УСТРОЙСТВА

Холсим позволява случайна лична употреба на предоставените от компанията ИТ устройства, доколкото тази употреба не е прекомерна или неподходяща и не води до разходи или вреди за Холсим или по друг начин не нарушава фирмените политики, закони или разпоредби.

Лични данни могат да се съхраняват на ИТ устройства на Холсим, включително в хранилището за документи на Холсим (в момента Google Drive), само доколкото количеството не е прекомерно, съдържанието не вреди на Холсим или по друг начин не нарушава фирмените политики, закони или разпоредби.

Личните данни, както и свързаните с компанията данни, съхранявани на платформите на Холсим, могат да бъдат пренасочени, прехвърлени или изтрити като част от процеса по напускане на служителя. Служителите носят отговорност за премахването на всички лични данни от платформите на Холсим преди да напуснат компанията. Холсим не носи отговорност за каквато и да е загуба на лични данни в резултат на напускането на служител или последващото пренасочване, прехвърляне или изтриване на данни.

Достъпът до уеб услугите на Холсим (напр. Google услуги на Холсим или публикувани приложения и услуги, достъпни по интернет) е възможен от всяко ИТ устройство (публично или лично) и е разрешен, доколкото потребителите спазват тази Директива. В такива случаи бизнес данните и документите, собственост на Холсим, могат да се копират на лични или други устройства, които не са собственост на Холсим, единствено за легитимна бизнес цел. Тези копия трябва незабавно да бъдат изтрити от устройството, след като бизнес целта вече не е валидна. На служителите е забранено да използват пълна синхронизация на хранилището за документи на Холсим (в момента Google Drive) на лични (различни от одобрените BYOD) или други устройства (напр. използване на „Google Drive for Desktop“ на личен лаптоп).

ПРАВИЛО 4: БЪДЕТЕ ВНИМАТЕЛНИ ОНЛАЙН. ПАЗЕТЕ СЕ ОТ РИСКОВЕ ЗА СИГУРНОСТТА ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ (AI), ИМЕЙЛ ИЛИ ИНТЕРНЕТ

Всички ИТ потребители са длъжни да използват имейл системата на Холсим (в момента „Gmail“) (а не лична имейл услуга) за служебни цели. При използване на имейл системата на Холсим трябва да се осигурят следните принципи:

- Изпращайте линкове към документи, вместо прикачени файлове.
- Не изпращайте съобщения до големи групи потребители, като например „All Users“ (Всички потребители).
- За външни имейли трябва да проверите двукратно дали имейлът или прикачените файлове не съдържат повече информация, отколкото е необходима на получателя.
- Имайте предвид, че всички имейли (включително вашите лични имейли, ако има такива), както и разговорите в Google Chat, се архивират по подразбиране за периода от време, дефиниран в съответствие с графика за съхранение на документи на Холсим, дори ако бъдат изтрити от входящата кутия, и могат да бъдат обект на преглед по време на разследвания, одити или други проверки (вижте по-долу). Google Chat и Google Spaces могат да се използват за комуникация с доставчици чрез прилагане на препоръките, включени в тази Директива.
- Платформата на имейл системата на Холсим включва възможност за директно докладване на СПАМ и фишинг имейли чрез бутона **„Phish Alert Button“**. Бързото докладване на такива подозрителни имейли ще помогне за по-ефективното филтриране в бъдеще.

Въпреки че използването на AI чатботове и LLM (големи езикови модели) инструменти предлага много ползи и възможности, то включва и определени рискове, които потребителите трябва да осъзнават и внимателно да управляват:

- Ако имате нужда от точни резултати, генерираният отговор трябва да бъде валидиран от експерт.
- Генерираният от AI текст за публикуване носи риск от нарушаване на авторски права.
- Използването на прекомерен контекст или честата смяна на темите може да доведе до „халюцинации“ (неправилни резултати).
- Ако са намесени лични данни, може да възникне риск от пристрастност (bias).

Когато използвате хранилището за документи на Холсим (в момента Google Drive), имайте предвид следните последици за сигурността:

- Използвайте хранилището за документи на Холсим за създаване и сътрудничество по документи.

- Всички документи, съхранявани в хранилището за документи на Холсим, са фирмени документи и се споделят само в съответствие с работните или функционалните изисквания. Всеки служител носи отговорност за лицата, на които предоставя достъп.
- Документите в хранилището за документи на Холсим могат да се споделят с временен достъп, за да се намали рискът от изтичане на данни.
- Когато работите с външни страни (напр. клиенти или доставчици), уверете се, че всички документи са създадени и съхранени в хранилището за документи на Холсим, за да се гарантира правилното им запазване.

ПРАВИЛО 5: ДОКЛАДВАЙТЕ ВСИЧКИ ИНЦИДЕНТИ СЪС СИГУРНОСТТА НА ИТ ОТДЕЛА

Инциденти с информационната сигурност са събития, показващи възможно нарушение на правилата за ИТ сигурност (дефинирани в тази Директива), отказ на контролни механизми или непозната досега ситуация, която може да е важна за сигурността (напр. фишинг имейли, споделяне на пароли, загуба или кражба на устройства, вируси и др.).

Всеки ИТ потребител трябва незабавно да докладва за инциденти със сигурността, проблеми и сривове, свързани с всяко ИТ устройство, приложение или ИТ-базирана услуга, на ИТ отдела и да следва предоставените след това инструкции.

По-долу са изброени някои често срещани и уместни инциденти със сигурността, заедно с препоръчителните действия, които трябва да се предприемат (неизчерпателен списък):

В случай на загуба или кражба на лаптоп или мобилно устройство:

- Незабавно се свържете с ИТ отдела, за да нулирате всички пароли.
- Своевременно докладвайте за загубата на вашия ръководител.
- В случай на кражба, незабавно докладвайте за инцидента в полицията.
- Подгответе опис на всички документи или данни, които може да са били изгубени или откраднати, и се уверете, че са предприети подходящи смекчаващи мерки, когато това е уместно за компанията.
- В случай на мобилни устройства, поискайте дистанционно изтриване на устройството (remote wipe) чрез ИТ отдела и докладвайте за загубата на телекомуникационния доставчик, след като ИТ отдела бъде информиран.

В случай на кликване върху фишинг имейл или съмнение за атака чрез социално инженерство:

- Незабавно спрете да взаимодействате с имейла, подателя, уебсайта, прикачения файл или обаждащия се.
- Докладвайте фишинг имейла с червения/оранжевия бутон *Phish Alert Button* в Gmail.
- Незабавно се свържете с ИТ отдела, променете паролите си и докладвайте върху какво е кликнато, каква информация е въведена и дали са изтеглени някакви файлове.

В случай на нарушение на сигурността на данните (data breach) или излагане на чувствителни данни:

- Докладвайте инцидента незабавно на ИТ отдела.
- Спрете споделянето, изпращането или модифицирането на засегнатите данни. Където е възможно, оттеглете достъпа до споделени файлове, линкове, папки или получатели.

- Не изтривайте файлове, имейли, съобщения в чата или лог файлове, свързани с инцидента.
- Идентифицирайте типа данни, които потенциално са засегнати (напр. данни за клиенти, данни за служители, финансови данни, идентификационни данни, поверителни документи).
- Запишете часа на излагането на данните, потенциалните получатели или страни с достъп и метода, по който е станало излагането.
- Не се опитвайте да скриете инцидента и не се свързвайте с външни страни, освен ако нямате разрешение за това.
- Сътрудничете на екипите по правни въпроси, съответствие (Compliance) и киберсигурност за мерките за локализиране и изискванията за уведомяване.

В случай на заразяване със зловреден софтуер (malware) или съмнение за компрометиране на системата:

- Незабавно се свържете с ИТ отдела и предоставете подробности за ситуацията. Предоставете възможно най-много информация, включително изпълнените файлове или наблюдаваното подозрително поведение. Променете незабавно всички пароли.
- Докладвайте за необичайно поведение, като изскачащи прозорци (pop-ups), съобщения от рансъмуер (ransomware), бавна производителност на системата, неоторизирани влизания, липсващи файлове или инсталиране на непознат софтуер.
- Оставете устройството включено, освен ако не е изрично инструктирано друго от ИТ отдела.
- Спрете да използвате засегнатата система незабавно. Не продължавайте да сърфирате, да изпращате имейли или да отваряте файлове.
- Не изтривайте файлове и не стартирайте инструменти за самопомощ за почистване или сканиране за вируси, освен ако не сте инструктирани да го направите от ИТ отдела.

ДРУГИ СЪОБРАЖЕНИЯ, КАСАЕЩИ ИТ ПОТРЕБИТЕЛИТЕ

Мониторинг, одити и разследвания

В съответствие с приложимите закони и разпоредби, стратегията за киберсигурност на Холсим има за цел да защити поверителността, целостта и наличността на информационните активи на Холсим, както и стабилността на нейната ИТ инфраструктура от широк спектър от вътрешни и външни заплахи, включително изтичане на данни, зловреден софтуер и неоторизиран достъп.

Целта на описаните тук дейности по мониторинг не е да се проучва поведението на служителите, тяхната производителност или поведение. Анализът, извършван от нашите инструменти за киберсигурност или системите за предотвратяване на загуба на данни (DLP), е фокусиран върху модели на данни, системни събития и нарушения на политиките, свързани с информационните активи. Той нито е предназначен, нито има за цел да прави заключения за представянето или работните навици на отделен служител, освен ако не е наложително официално разследване на инцидент със сигурността. В съответствие с принципа на прозрачност, всички служители на Холсим с настоящото се информират, че дейностите по мониторинг, подробно описани в този раздел, са внедрени в корпоративната ИТ среда. Настоящата Директива служи като основно и постоянно средство за уведомяване за тези дейности.

Служителите запазват пълните си законни права, включително правото да изискват информация относно обработваните за тях лични данни. Такива искания трябва да бъдат адресирани до определеното длъжностно лице по защита на данните (DPO) или Правния отдел и отдела за нормативно съответствие (Legal and Compliance).

Оторизирани дейности за предотвратяване на загуба на данни и мониторинг на киберсигурността – превантивен и детективен контрол

Стратегията на Холсим за киберсигурност и DLP е изградена върху балансиран и многослоен модел на защита, който използва както превантивен (Preventive), така и детективен (Detective) контрол. Този подход гарантира многослойна защита (defense-in-depth), където множество нива на сигурност работят в синхрон за защита на нашите активи от данни.

Като част от тази стратегия, отговорният ИТ отдел е инструктиран и има право да извършва превантивен и детективен мониторинг на лог файловете на ИТ системите, заедно с отчети, за да осигури защитата на фирмените данни и спазването на правилата в тази Директива и приложимите закони или разпоредби.

- **Превантивен контрол:** Това са проактивни мерки, интегрирани в нашите системи и процеси, предназначени да спрат инциденти със загуба на данни, преди те да възникнат. Те представляват нашата първа линия на защита. Примерите включват стабилни системи за контрол на достъпа, които налагат принципа на минималните привилегии, задължително криптиране на данни за чувствителни файлове и политики, които блокират трансфера на данни към неоторизирани дестинации.

- **Детективен контрол:** Това са реактивни мерки, предназначени да идентифицират инциденти със загуба на данни, които или са заобиколили превантивния контрол, или в момента се изпълняват. Те служат като критична втора линия на защита, позволяваща бързо разследване и реагиране. Примерите включват анализ на системните лог файлове за аномална активност, сигнали в реално време за нарушения на политиките и редовни одити на сигурността.

Въпреки че превантивният контрол е предпочитаният метод за смекчаване на риска, детективният контрол е незаменим. Той осигурява необходимата видимост, за да се потвърди, че превантивните мерки функционират по предназначение, и да се открият сложни или нови опити за заобикалянето им. Комбинацията от двата вида контрол, съгласно примерите по-долу (неизчерпателен списък), създава устойчива екосистема за сигурност:

Дейност по мониторинг	Описание	Основна цел
Анализ на изтеглянето на данни	Мониторинг на обема, честотата и вида на данните, изтеглени от корпоративните хранилища (напр. SharePoint, Google Drive, мрежови файлови сървъри) към устройствата на потребителите. Анализът се фокусира върху метаданни и модели.	За откриване на необичайни модели на агрегиране на данни, които могат да показват неоторизирано събиране на данни с цел извличане (exfiltration).
Сканиране на изходящи имейли	Анализ на изходящи имейли и техните прикачени файлове, изпратени от акаунт на Холсим до външен получател.	За предотвратяване на случайно или зловредно изтичане на ограничена (Restricted) или поверителна (Confidential) информация чрез имейл, който е основен вектор за загуба на данни.
Преглед на лог файловете за потребителски достъп	Мониторинг и одит на събития за потребителска автентификация (влизания, неуспешни влизания) и събития за достъп в интернет, критични системи, приложения и бази данни.	За осигуряване на спазването на принципа на минималните привилегии, откриване на опити за неоторизиран достъп, идентифициране на компрометирани идентификационни данни и разследване на потенциално ескалиране на привилегии или компрометиране.
Контрол на сменяеми носители	Мониторинг и, когато е необходимо, ограничаване или блокиране на използването на USB флаш памети, външни хард дискове и други сменяеми носители или устройства за	За предотвратяване на неоторизиран трансфер на чувствителни данни на Холсим към незащитени, неуправлявани и лесно губещи се или крадени лични устройства.

Дейност по мониторинг	Описание	Основна цел
	съхранение на данни на корпоративни крайни устройства.	
Мониторинг на облачни приложения	Мониторинг на трансфера на данни към и от одобрени корпоративни облачни услуги и неодобрени облачни услуги за масово ползване.	За предотвратяване на извличането на корпоративни данни към неоторизирани лични или чужди платформи за облачно съхранение, които попадат извън контрола за сигурност на Холсим.

СПЕЦИФИЧЕН МОНИТОРИНГ НА ДАННИ И СИСТЕМИ

Мониторинг на трансфера на данни и крайните устройства (Данни в употреба/в движение)

- **Обем на изтегляне на данни:** ИТ отделът ще наблюдава системно генерираните лог файлове от нашите централни хранилища за данни, включително Google Drive, сайтове на SharePoint, акаунти на OneDrive за Business и мрежови файлови сървъри, за да анализира обема на данните, изтеглени към крайните устройства на потребителите. DLP системата е проектирана да установи базова линия (baseline) за нормална дейност при достъп до данни. След това тя ще генерира автоматични сигнали, когато бъдат открити значителни отклонения от тази базова линия, като например необичайно голям обем изтегляния за кратък период, което може да показва масово събиране на данни в подготовка за извличане.
- **Сменяеми носители:** За да се смекчи значителният риск, произтичащ от преносимите памети, използването на USB устройства, външни хард дискове и други сменяеми носители може да бъде наблюдавано, ограничено или напълно блокирано на корпоративните крайни устройства.

Мониторинг на оторизацията и достъпа на потребителите (Данни в употреба)

ИТ отделът непрекъснато ще наблюдава и периодично ще преглежда лог файловете за всички критични бизнес приложения, бази данни, файлови сървъри и инфраструктурни компоненти. Този мониторинг включва систематичен преглед на достъпа на потребителските акаунти до данни, включително местата и часовете на достъп.

Основната цел на тази дейност е да се потвърди, че нашите технически контроли за достъп функционират правилно и че се спазва принципът за достъп с минимални привилегии, според който на лицата се предоставя достъп само до конкретните данни и системи, необходими за изпълнение на техните работни функции.

Специфичните наблюдавани събития включват успешни и неуспешни опити за влизане, достъп до чувствителни файлове извън нормалното работно време и всякакви промени в потребителските разрешения или членството в групи в рамките на системите за управление на идентичността като Active Directory. Този детективен контрол е жизненоважен за идентифициране на потенциални заплахи за сигурността, като атаки с груба сила срещу пароли (brute-force attacks), използване на компрометирани идентификационни данни или вътрешни опити за неоторизирано ескалиране на привилегии.

Този обхват на мониторинг покрива достъп, произхождащ от всички устройства, включително както корпоративно оборудване, управлявано от Холсим, така и лични устройства, за които изрично е предоставен достъп до корпоративни данни.

Мониторинг на електронните комуникации (Данни в движение)

- **Анализ на изходящи имейли:** DLP системата на Холсим може автоматично и програмно да сканира имейли и техните прикачени файлове, изпратени от корпоративен имейл акаунт на Холсим до външен получател.
- **Важно ограничение:** Този мониторинг е автоматизиран и независим от съдържанието (content-agnostic), като се фокусира върху обективни модели на данни, а не върху субективната същност или значение на комуникацията. Този процес не се прилага за вътрешни имейл комуникации между потребители на Холсим. В юрисдикции, където е разрешено ограничено лично използване на корпоративен имейл от местна политика, системата е конфигурирана да зачита принципа на тайната на кореспонденцията. Човешки преглед на всеки маркиран имейл може да се извършва само като част от официално разследване, уредено от протокола за реагиране при инциденти или вътрешния процес на разследване.

Ad-Hoc и целеви мониторинг

Холсим си запазва правото при специфични и контролирани обстоятелства (напр. включително, но не само, за служители в предизвестие) и в съответствие с приложимите закони и разпоредби, да прилага по-насочен, неанонимен мониторинг на дейността на отделен потребител в ИТ системите.

ОДИТИ, РАЗСЛЕДВАНИЯ И ДРУГИ ПРОВЕРКИ

Всички данни, използвани и съхранявани:

- във връзка с използването на ИТ услуги на Холсим (включително информация за лични устройства, свързани с ИТ системата на Холсим), или
- на лични устройства или на предоставени или одобрени от компанията устройства, включително информация, съдържаща се в лично управлявани приложения за съобщения (напр. като WhatsApp, Telegram, Signal и др.),

могат да бъдат подложени на скрининг на данни и криминалистични процедури във връзка с разследвания за нормативно съответствие (compliance) или прегледи за лоялна

конкуренция, както и други процеси с цел защита на легитимните интереси на компанията.

Такъв скрининг на данни ще се придържа към приложимите закони и разпоредби, както и към професионалните и етичните стандарти, изложени в тази Директива или всякакви други съответни политики и разпоредби на Холсим.

При поискване служителите са длъжни да предоставят устройствата си според инструкциите на ИТ отдела или на други лица, посочени от Правния отдел и отдела за съответствие. Изтриването на данни от предоставено от компанията или лично ИТ устройство (включително данни в услуги за съобщения) след уведомяване за или по друг начин научаване за одит, разследване или друг преглед е забранено и може, в зависимост от обстоятелствата, да се счита за нарушение на тази Директива, подлежащо на санкции.

ПЕТ ПРАВИЛА ЗА ИНФОРМАЦИОННА СИГУРНОСТ ЗА СЛУЖИТЕЛИ

ИНФОРМАЦИОННАТА СИГУРНОСТ НА МОЕТО РАБОТНО МЯСТО Е МОЯ ОТГОВОРНОСТ

ПРАВИЛО 1: ПАЗЕТЕ ПАРОЛИТЕ СИ В ТАЙНА И ЗАКЛЮЧВАЙТЕ ЕКРАНА НА КОМПЮТЪРА СИ

ПРАВИЛО 2: НЕ ИНСТАЛИРАЙТЕ НИКАКЪВ СОФТУЕР ИЛИ ХАРДУЕР НА ВАШАТА СИСТЕМА БЕЗ КОНСУЛТАЦИЯ С ИТ ОТДЕЛА

ПРАВИЛО 3: ПАЗЕТЕ ВАШИТЕ ИТ УСТРОЙСТВА И ИНФОРМАЦИОННИ АКТИВИ ОТ ПОВРЕДА ИЛИ ЗАГУБА

ПРАВИЛО 4: БЪДЕТЕ ВНИМАТЕЛНИ ОНЛАЙН. ПАЗЕТЕ СЕ ОТ РИСКОВЕ ЗА СИГУРНОСТТА ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ (AI), ИМЕЙЛ ИЛИ ИНТЕРНЕТ

ПРАВИЛО 5: ДОКЛАДВАЙТЕ ВСИЧКИ ИНЦИДЕНТИ СЪС СИГУРНОСТТА НА ИТ ОТДЕЛА

Прочетох и разбрах Директивата за потребителите на информационни системи на Холсим, както и 5-те правила, които обобщават нейното съдържание. Ще спазвам 5-те правила по всяко време. Наясно съм, че неспазването на тези правила може да доведе до финансови и репутационни щети за Холсим и до дисциплинарни действия.

Име на служителя: _____

Дата: _____

Подпис: _____

ПЕТ ПРАВИЛА ЗА ИНФОРМАЦИОННА СИГУРНОСТ ЗА ВЪНШНИ ФИРМИ

ИНФОРМАЦИОННАТА СИГУРНОСТ НА МОЕТО РАБОТНО МЯСТО Е МОЯ ОТГОВОРНОСТ

ПРАВИЛО 1: ПАЗЕТЕ ПАРОЛИТЕ СИ В ТАЙНА И ЗАКЛЮЧВАЙТЕ ЕКРАНА НА КОМПЮТЪРА СИ

ПРАВИЛО 2: НЕ ИНСТАЛИРАЙТЕ НИКАКЪВ СОФТУЕР ИЛИ ХАРДУЕР НА ВАШАТА СИСТЕМА БЕЗ КОНСУЛТАЦИЯ С ИТ ОТДЕЛА

ПРАВИЛО 3: ПАЗЕТЕ ВАШИТЕ ИТ УСТРОЙСТВА И ИНФОРМАЦИОННИ АКТИВИ ОТ ПОВРЕДА ИЛИ ЗАГУБА

ПРАВИЛО 4: БЪДЕТЕ ВНИМАТЕЛНИ ОНЛАЙН. ПАЗЕТЕ СЕ ОТ РИСКОВЕ ЗА СИГУРНОСТТА ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ (AI), ИМЕЙЛ ИЛИ ИНТЕРНЕТ

ПРАВИЛО 5: ДОКЛАДВАЙТЕ ВСИЧКИ ИНЦИДЕНТИ СЪС СИГУРНОСТТА НА ИТ ОТДЕЛА

Прочетох и разбрах Директивата за потребителите на информационни системи на Холсим, както и 5-те правила, които обобщават нейното съдържание. Ще спазвам 5-те правила по всяко време. Наясно съм, че неспазването на тези правила може да доведе до финансови и репутационни щети за Холсим и моята собствена компания, което потенциално може да доведе до прекратяване на услугите, предоставяни на Холсим.

Име на служителя: **Име на фирмата:**

_____

Дата: **Подпис:**

УПРАВЛЕНИЕ НА ДОКУМЕНТА	
Одобрено от	Главен директор по информационна сигурност (CISO)
Свързани политики, директиви и MCS	Политика за информационни технологии Директива за съхранение и изтриване на данни Директива за изкуствен интелект MCS 36, MCS 37, MCS 38, MCS 39, MCS 40
Други поддържащи документи	Глобален стандарт за ИТ сигурност Ръководство за класификация на информацията Процедура за класификация на информацията Шаблон „Пет правила за информационна сигурност за служители“ Шаблон „Пет правила за информационна сигурност за външни фирми“ Списък с контакти- Service Desk

КОНТРОЛ НА ВЕРСИИТЕ			
Номер на версията	Дата на издаване	Автор	Резюме на промените
Версия 2.0	22 октомври 2020 г.	CDIO, CISO	Актуализация на директивата въз основа на най-добрите практики за изискванията за пароли, жизнения цикъл на данните и управлението на софтуера от Директивата за потребителите на ИТ информационни системи (февруари 2016 г.).
Версия 2.1	8 декември 2020 г.	CISO	Подробно специфицирани изисквания за пароли, отново са добавени 5-те правила (Произход: първа версия от 2016 г.).

УПРАВЛЕНИЕ НА ДОКУМЕНТА			
Версия 2.1.1	8 декември 2021 г.	CISO	Преглед, козметични промени.
Версия 2.2	4 април 2024 г.	DMO, CISO	Преглед, промени (разяснения) в „Управление на документи и данни“ относно използването на AI и други облачни услуги на трети страни; разделът за разследвания е преформулиран, за да бъде в съответствие с „Меморандума Монако“ (Monaco Memo).
Версия 2.3	23 юли 2025 г.	DMO, CISO	Разяснения относно използването на приложения за съобщения; актуализации относно AI; интегриране на управлението за предотвратяване на загуба на данни (DLP).
Версия 2.4	15 май 2026 г.	CISO	Структурни и съдържателни актуализации, включително установяването на Петте правила за информационна сигурност, сигурен мениджър на пароли за Холсим, дейности по мониторинг в рамките на ИТ, използване на неподдържан или забранен софтуер, инструменти за отдалечен достъп, увеличена дължина на ПИН кода за мобилни устройства. Допълнителни насоки за докладване на инциденти със сигурността и насоки за класификация на данните.