ИНФОРМАЦИОННА СИГУРНОСТ
как да обезпечиш поверителност на данните

www.NFTINI.org

Сигурност е функционалното състояние на дадена система, обезпечаващо успешно противодействие срещу и по възможност неутрализиране на фактори и обстоятелства, насочени към или от естеството да въздействат деструктивно или да влияят неблагоприятно на самата система или на фактори и обстоятелства, от които системата зависи.

> **Абсолютна сигурност не съществува.** Следователно информационната сигурност предполага защита до такава степен, че да е неудобно, неизгодно, обезсърчаващо да се правят опити да се достигне до данните; да не си струва да се вложат такива усилия, които са необходими за преодоляване на съществуващите защити.

Обезпечаването на една **система за сигурност** изисква съблюдаването на такива принципи:

- **комплексност** – постигане на всеобхватност, гарантираща сигурността „от всички страни“, като отчита всички критични фактори и елементи;
- **простота** – включване в системата на възможно най-малък брой, възможно най-прости елементи, от които сигурността да зависи;
- **независимост** на системата от елементи, които не са под наш контрол или не могат бързо, лесно, надеждно да се поставят под наш контрол;
- **алтернативност** – ваимозаменяемост на елементите в системата, които са критични за нейното правилно и стабилно функциониране;
- **балансираност** – обезпечаване на „достатъчно“ сигурност в системата, в зависимост от размера на рисковете и от вероятността да настъпят;
- **динамичност** – постоянен преглед и бързо обновяване на системата в зависимост променящите се условия и нововъзникващите заплахи;
- **перспективност** – усъвършенстване на концепциите за сигурност при отчитане на съществуващите тенденции и предстоящи събития.

Информационната сигурност включва необходимия комплекс от организационни и технически мерки, които са в състояние в конкретния случай да обезпечат дължимата поверителност на данните и недопускане на тяхното неразрешено / нежелано прочитане, копиране, променяне или унищожаване.

> Сред най-важните данни, които твоята **Синдикална секция** обработва, са личните данни на **синдикалните членове**. Понякога Работодателите злоупотребяват със своите права осъществяват съвсем целенасочен тормоз спрямо тях – поради което може да се окаже целесъобразно да бъде запазено в дълбока тайна кой симпатизира на синдикатите и кой членува в тях. В тази връзка не случайно председателят и секретарят (които в повечето случаи са известни на Работодателя) се ползват от законова закрила срещу дисциплинарно уволнение и освобождаване поради съкращаване на щата.
>
> Други важни тайни, чиято сигурност трябва да бъде обезпечена, са свързани с информацията, която Работодателят е длъжен да предостави на синдикатите при **колективни трудови преговори** и при осъществяване на цялостния **социален диалог**. Често тази информация включва фирмени тайни, подробности от финансовото състояние на предприятието, планове за предстоящи преструктурирания и други – които не желаем да попаднат в ръцете на конкуренцията и да навредят на нашите Работодатели!

Не рядко синдикатите се налага да работят с данните по конкретни **сигнали за нередности** или с тези по предстоящи, текущи или приключили **съдебни дела** (най-често на наши синдикални дейци или на трудовия колектив като цяло срещу Работодателя). Преждевременното разкриване на такива данни може да затрудни установяването на обективната действителност или да навреди неоснователно на Работодателя.

Опазването на тайната е съществено и при подготвянето и провеждането на **ефективна стачка** – където изненадата често се оказва решаващ фактор, а поставените искания и водените преговори в повечето случаи засягат репутацията и търговските тайни на Работодателя.

И не на последно място – синдикалните дейци почти постоянно получават, обработват и предават към свои колеги данни, свързани с вътрешния синдикален живот на нашите структури – свързани с разглеждане **предложенията** от организационен и практически характер, **гласуването** при избор на синдикални лидери или очертаване на синдикални политики, **участието** в конкретни инициативи на синдикатите.

Организационните мерки за информационна сигурност включват действия, отношения с хора, принципни начини на работа. Трудно могат да се дадат изчерпателни указания (всеки конкретен случай може да е специфичен), но обикновено следните насоки могат да бъдат полезни:

- **Не клюкарствай.** В повечето случаи безцелното споделяне на информация не е продуктивно, а понякога казаното само на едного (включително с уговорка *„да не казва на никого“*) може да се разбере от всички; или дори да се разбере нещо изопачено, преувеличено, изобличаващо.

- **Спазвай процедурите.** Дадени теми не трябва да се обсъждат извън определени кръгове. Въпросите от вътрешния синдикален живот са само за синдикалисти. Ако преговаряте по някакъв повод с Работодателя, разкривай на трети страни само такава информация, която няма да засегне никого от преговарящите.

- **Не смесвай каналите.** Ако трябва да споделиш например някаква синдикална тайна, може би служебните помещения не са най-доброто място; нито служебният телефон (компютър); нито служебната електронна поща. Поддържай независими канали за поверителната информация.

- **Поддържай ред.** Ако работиш с документи (били на хартия, били в електронна среда), е добре да знаеш всеки от тях къде се намира и защо е точно там. Освен че така ще можеш да работиш по-бързо и ефективно, ще можеш да имаш едно на ум в кои документи има поверителна информация и трябва да бъдат държани на сигурно място.

- **Не копирай безцелно.** Не размножавай и не разпространявай поверителна информация без причина. Създаването на множество копия може да доведе до изгубване на някое от тях или до пропускане да бъде унищожено след като вече не е необходимо. Освен това всяко следващо копие е „още един риск“ от разкриване на поверителната информация.

- **Внимавай при пренасянето.** Ако се налага да пренасяш поверителни документи на хартия или електронни носители с памет, обмисли предварително маршрута, избери безопасна част на деня и вземи със себе си придружители. Постарай се информацията да бъде доставена възможно най-бързо до своето сигурно местоназначение.

- **Минимизирай данните.** Не дръж при себе си информация, която не е необходима. Документи, които трябва да бъдат предадени накому, предай възможно най-рано. Документи, които вече не

са необходими, унищожи по най-бързия начин. Ако нещо не е необходимо да се документира или да се казва, просто го остави да отлети и да се забрави.

- **Дръж нещата под ключ.** Без значение дали са на хартия или в електронна среда, документите с поверителна информация не бива да остават лесно достъпни за трети страни (освен ако това не е необходимо). Дръж хартиените документи заключени (или ги скрий на някое неочаквано място). Шифровай електронните документи или поне ги архивирай в директория с парола. И вземи мерки срещу неразрешено влизане в компютъра, където ги съхраняваш.

- **Обучавай се.** Добра идея е да следиш новостите в информационната сигурност и да ги прилагаш, когато това е уместно. Ефективните мерки днес могат да бъдат компрометирани утре и да са необходими други мерки. Полагай усилия и твоите колеги да актуализират представите си за това какви мерки са необходими.

Във връзка с горните организационни мерки трябва да знаеш, че каквото и да разкриеш пред нашите синдикални дейци, то е **служебна тайна** по силата на чл. **403**, ал. **1**, т.т. **1** и **2** във вр. с чл. **406**, ал. **3** от **Кодекса на труда**. Ако ползваш съдействието на адвокат (било в синдикалната организация, било другаде), всичко казано помежду ви е **адвокатска тайна** – то не може да бъде узнавано, записвано и използвано от трети лица по никакъв повод. Дори да представлява доказателство за извършени престъпления и да включва направени самопризнания, то не може да бъде приложено като доказателство (освен като доказателство за това, че този, който го разкрива, е нарушил адвокатската тайна и подлежи на санкция за това). Но въпреки тези законови гаранции, имай едно на ум винаги, когато мислиш да кажеш / напишеш някоя тайна и не пренебрегвай дадените насоки.

Техническите мерки за информационна сигурност включват осигуряването на инфраструктура, технологии и подходи. Трудно могат да се дадат изчерпателни указания (всеки конкретен случай може да е специфичен), но обикновено следните насоки могат да бъдат полезни:

- **Заключвай старателно.** Съхранявай хартиените документи и електронните носители с памет по възможност в заключено помещение, където само ти имаш достъп. По възможност ползвай метален шкаф със заключващо устройство. Ако не разполагаш с такива условия, помисли какво можеш да пригодиш за целта.

- **Ползвай само лицензиран софтуер.** Не разчитай на „кракнати“ версии на софтуер, който изисква валиден лиценз. Никой не може да гарантира как точно е „кракнат“ такъв софтуер и доколко надеждно функционира. Ако не желаеш да плащаш за необходимия ти софтуер, дали не е добра идея да се запознаеш с концепцията за **Свободен софтуер**?

- **Ползвай само надежден софтуер.** „Надежден“ е само този софтуер, който ти позволява да знаеш как работи; и не те прави зависим от конкретна разработваща компания. Несвободният софтуер (какъвто е **Windows**, **MacOS**, **iOS** и дори **Android**) не е надежден, защото там не можеш да знаеш как работи софтуерът и си напълно зависим/а от разработващата компания (която единствена има право да променя софтуера). С такъв софтуер не можеш да гарантираш кой знае каква сигурност на информацията. Ако не желаеш да ползваш софтуер, за който дори нямаш право да знаеш какво прави на собствения ти компютър / телефон, дали не е добра идея да се запознаеш с концепцията за **Свободен софтуер**?

- **Ползвай само твои ресурси.** Работодателят често си запазва правата на администратор спрямо служебните устройства, сървъри, облачни услуги; това му позволява да преглежда

съдържанието, да „подслушва“ разговорите, да блокира достъпа. Не ползвай служебни ресурси за съхраняването или предаването на каквато и да било поверителна информация.

- **Ползвай сигурна парола.** Не е добра идея паролата ти да е свързана с името ти, рождената ти дата, телефонния ти номер; да е кратка, само с малки букви, само с цифри, без специални символи; да е записана на листче до компютъра ти; да същата като за други ресурси в internet; да не е променяна от години; да е споделена *„с една много добра приятелка“*.

- **Шифровай.** Макар да е трудно (освен ако не се занимаваш с такива неща), е много полезно да се запознаеш с **асиметричното шифроване**, което ти позволява да предаваш сигурно информация на трети страни, включително и без да сте разменили тайно шифровъчни ключове. Отличен **Свободен софтуер** за тази цел е **GnuPG**.

Във връзка с горните технически мерки трябва да знаеш, че съвременната криптография е достигнала до много високи нива на сигурност, „най-слабото звено“ в които е твоята парола. Ако базираш твоята информационна сигурност на **Свободни софтуерни технологии** (които се поддават на независима проверка за начина им на функциониране и могат да бъдат усъвършенствани от всеки доверен лично на теб програмист), можеш да постигнеш респектиращи нива на **информационна сигурност**. При все обаче трябва да имаш едно на ум, че **абсолютна сигурност** (**особено в електронна среда**) **няма**. Ако не е наистина необходимо, не въвеждай поверителна информация в електронна среда. И унищожавай всички поверителни файлове и документи (били на хартия, били в електронна среда), веднага след като вече не са наистина необходими.

Не се ограничавай до настоящите напътствия! Информационната сигурност е комплексен и динамичен въпрос; обхваща многобройни фактори и се изменя постоянно във времето с напредъка на науката и техниката. Запознавай се с новостите и ги въвеждай своевременно.

Информационната сигурност не е само индивидуален въпрос. Запознай колегите си с настоящите напътствия и изисквай от тях да спазват разумни нива на дисциплина, за да запазят поверителната информация, която им споделяш. Защото колкото и високи нива на информационна сигурност да поддържаш, това няма да има никакъв ефект, ако информацията „изтича“ от твоите партньори.