ЗАШТИТА ТАЈНИХ ПОДАТАКА У ДИГИТАЛНОЈ СФЕРИ ЗАБРАЊЕНЕ ПРАКСЕ

Зашто је тема важна? - Заштита тајних података у дигиталној сфери није бирократска формалност нити пуко технолошко питање, већ темељ националне безбедности. Један непромишљен поступак може довести до озбиљних последица по државу и грађане.

Најчешће забрањене праксе

1. **Слање докумената преко апликација за брзу комуникацију** (Viber, WhatsApp, Signal) → неконтролисан пренос, висок ризик цурења.
2. **Разговори о тајним подацима преко мобилних телефона и отворених линија** → могућност прислушкивања.
3. **Коришћење система електронске писарнице** (нпр. еУправа) → нису сертификовани за рад са тајним подацима.
4. **Креирање докумената на рачунару повезаном на интернет, Wi Fi или несертификовану интерну мрежу** → изложеност сајбер нападима.
5. **Коришћење приватних лаптопова, рачунара и мобилних телефона за обраду, чување или пренос тајних података** → неконтролисани системи, без безбедносних мера.
6. **Коришћење приватних USB меморија и преносивих медија** → неконтролисан пренос, ризик од малвера.
7. **Постављање фотографија, снимака екрана или садржаја који садржи тајне податке на друштвеним мрежама** (Telegram, X/Twitter, TikTok, Facebook, Instagram и др.) → неконтролисано ширење, трајни губитак тајности.
8. **Размена података путем приватних имејл налога** (Gmail, Yahoo, Outlook.com) → непоуздана заштита, ризик компромитације.
9. **Чување докумената у комерцијалним cloud сервисима без одобрених државних или сертификованих система** (Google Drive, Dropbox, iCloud) → неконтролисан приступ, могућност злоупотребе.
10. **Коришћење отворених видеоконференцијских платформи за разматрање или размену тајних података** (Zoom, Teams, Meet) → потенцијалне безбедносне рупе и прислушкивање.
11. **Унос, копирање или постављање тајних података у јавно доступне системе генеративне вештачке интелигенције** (ChatGPT, Gemini, Copilot и др.) → губитак контроле над подацима, могућност њихове анализе, чувања и неовлашћене употребе.
12. **Аутоматска синхронизација службених докумената са приватним cloud налозима** → губитак контроле над тајним подацима.
13. **Повезивање службених уређаја на јавне Wi Fi мреже** → повећан ризик од пресретања комуникације и сајбер напада.

ЗАШТИТА ТАЈНИХ ПОДАТАКА У ДИГИТАЛНОЈ СФЕРИ
ЗАБРАЊЕНЕ ПРАКСЕ

Додатне критичне грешке

- **Штампање докумената на мрежним или заједничким штампачима** → могућност неовлашћеног приступа и губитка контроле над копијама.
- **Фотографисање екрана или радног места мобилним телефоном** → неконтролисано ширење тајних података.
- **Рад са тајним подацима ван одобрених службених просторија** (рад од куће, јавни простори, хотели) → немогућност обезбеђивања прописаних мера заштите.
- **Дељење екрана током видео састанака без провере садржаја** → ненамерно откривање тајних података.
- **Достављање података лицима која немају потребу да знају** („need to know“ – принцип „потребе да се зна“) → неовлашћено откривање информација.
- **Остављање откључаног рачунара или незаштићених медија без надзора** → могућност неовлашћеног приступа.
- **Чување лозинки на папирићима или у незаштићеним документима** → компромитација приступних података.
- **Инсталирање неовлашћеног софтвера** (Shadow IT) → ризик од крађе података.
- **Фишинг и социјални инжењеринг** → отварање сумњивих линкова и прилога доводи до компромитације система.
- **Неправилно уништавање тајних података** → обавезно коришћење сигурносних шредера или софтверског брисања по стандардима.

Шта уместо тога?

Забрањено	Дозвољено
Viber, WhatsApp	Сертификовани системи за размену тајних података
Gmail, Yahoo	Службене имејл адресе са криптографском заштитом
Google Drive, iCloud	Сертификовани системи за складиштење (државни дата центар)
Zoom, Teams, Meet	Сертификовани системи за видео конференције
Приватни USB	Сертификовани медији са енкрипцијом

ЗАШТИТА ТАЈНИХ ПОДАТАКА У ДИГИТАЛНОЈ СФЕРИ
ЗАБРАЊЕНЕ ПРАКСЕ

Пример из праксе: У пракси је забележен случај где је једно лице фотографисало екран са тајним податком и послало га преко WhatsApp а колеги. Фотографија је ненамерно завршила у групном ћаскању, што је довело до покретања дисциплинског поступка и новчане казне.
Поука: Никада не користити приватне апликације или уређаје за пренос тајних података.

Одговорност руководилаца: Руководиоци су дужни да обезбеде услове за безбедан рад са тајним подацима, организују редовне обуке запослених и врше надзор над применом прописаних мера заштите. Пропуст у надзору може довести до њихове личне одговорности.

Правна напомена: Наведене праксе представљају тешко кршење мера заштите тајних података и могу довести до дисциплинске, прекршајне или кривичне одговорности, у складу са Законом о тајности података, Кривичним закоником Републике Србије и подзаконским актима.

Пријављивање инцидента: У случају сумње да је дошло до компромитације тајних података, сваки запослени је дужан да без одлагања обавести непосредног руководиоца и лице задужено за заштиту тајних података. Брза реакција значајно смањује последице безбедносног инцидента.

Запамтите: Сваки пропуст – било дигитални или физички – може постати озбиљан ризик по националну безбедност или безбедносни инцидент. Свако лице које рукује тајним подацима лично је одговорно за њихову заштиту. Ако нисте сигурни – питајте. Ако сте направили грешку – одмах пријавите. Тишина није заштита – тишина је ризик.

Безбедност нема алтернативу.