

**Cilj:**

Na prvi pogled vidjeti koje informacije idu u ormar za dokumente, sef ili podatkovni sef, što treba uništiti i gdje je korisna digitalna kopija.

01

Ormar za dokumente – Za povjerljive dokumente koji su redovito potrebni.

Tipični sadržaji:

- Kadrovski dokumenti poput ugovora o radu, ocjena ili bolovanja – moraju biti sigurni, ali brzo dostupni.
- Financijski i računovodstveni dokumenti poput računa, bilanci ili poreznih dokumenata koji se redovito obrađuju.
- Tekući ugovori s kupcima, dobavljačima i partnerima – pristup treba biti jasno uređen.
- Interne smjernice, operativne, sigurnosne i radne upute, kako bi svakodnevica tekla bez zastoja.

Osnovna pravila:

- Ormar uvijek držati zaključanim; ključeve ili pristup dati samo ovlaštenim osobama.
- Dokumente razvrstati tematski i pohraniti prema roku čuvanja, kako bi se izbjegli nered i vrijeme traženja.
- Istekle dokumente redovito premještati u zaštićene spremnike za uništavanje dokumenata, kako bi se smanjili rizici zaštite podataka.

02

Sef / sigurnosni ormar – Za posebno vrijedne ili kritične sadržaje.

Tipični sadržaji:

- Izvorne isprave poput osnivačkih dokumenata, zemljišnoknjižnih izvadaka ili javnobilježničkih ugovora, čiji bi gubitak imao pravne posljedice.
- Mape za potpis, pečati tvrtke i punomoći koji su operativno neophodni.
- Nosači podataka s osjetljivim informacijama, poput diskova za sigurnosne kopije, USB memorija ili povjerljivih projektnih medija.
- Vrijednosti poput gotovine, bonova ili osjetljivog hardvera (npr. pristupnih tokena).

Osnovna pravila:

- Sef čvrsto usidriti i postaviti u zaštićeno, nenametljivo područje, kako bi se otežale manipulacije.
- Jasno definirati prava pristupa; ne "svi zaposlenici s ključem".
- Dokumentirati pristupe, npr. kroz evidencije zaključavanja ili popise pristupa, kako bi odgovornost ostala sljedeća.

03 Podatkovni sef / protupožarni ormar za nosače podataka – Za medije osjetljive na toplinu i vlagu.

Tipični sadržaji:

- Sigurnosne kopije ERP, HR ili proizvodnih sustava, čija je obnova u hitnom slučaju kritična.
- Posebni nosači podataka poput traka, SSD-ova ili vanjskih diskova, osobito osjetljivi na toplinu i vlagu.
- Arhivirani projektni podaci koji su pravno ili operativno relevantni.

Osnovna pravila:

- Koristiti samo provjerene ormare za nosače podataka (prilagođene klase vatre i temperature).
- Redovite sigurnosne kopije rotirati prema fiksnoj shemi (dnevno, tjedno, mjesečno), kako bi se izbjegao gubitak podataka.
- Nosače podataka jasno označiti (sadržaj, datum, sustav) – za brzu obnovu i pregled.

04 Što se uništava? – Pravilno koristiti uništavače dokumenata i digitalno brisanje.

Papirnati dokumenti:

- Osobni podaci (prijave, stari kadrovski dosjei, platne liste).
- Zastarjeli ugovori, ponude ili kalkulacije s povjerljivim informacijama.
- Ispisi s pristupnim podacima, internim strategijama ili financijskim informacijama.
- Bilješke, zapisnici i međustanja koja sadrže osjetljive detalje.

Osnovna pravila:

- Odabrati sigurnosnu razinu prema potrebi zaštite – više razine za HR i financijske podatke.
- Spremnike za prikupljanje zaključavati i redovito prazniti, kako bi se osiguralo potpuno uništenje.

Digitalni podaci:

- Zastarjele sigurnosne kopije koje više nisu potrebne.
- Nosači podataka na kraju životnog vijeka (neispravni diskovi, USB memorije, trake).
- Testni podaci ili kopije koji sadrže osjetljive sadržaje.

Savjet: I digitalno, prava pristupa trebaju biti jasno uređena, a procesi brisanja dokumentirani.

05 Kombinirati fizičko čuvanje + digitalnu sigurnosnu kopiju

Osnovno načelo: Važne informacije čuvaju se fizički sigurno i digitalno sigurnosno kopiraju – nikada nekontrolirano dupliciraju.

Primjeri:

- ▶ **Važni ugovori:** Izvornik u ormaru za dokumente ili sefu, skenirana verzija u revizijski sigurnoj digitalnoj arhivi.
- ▶ **Kritični operativni i pogonski podaci:** Radna verzija u sustavu, redovita sigurnosna kopija u podatkovnom sefu ili sefu.
- ▶ **Kadrovski i HR podaci:** Papirnati dokumenti u ormaru za dokumente, digitalni dosjei u zaštićenom sustavu s upravljanjem pravima.

Savjet: Fizička i digitalna sigurnost nadopunjuju se – tako izbjegavate gubitak podataka, krađu ili slučajnu objavu.

06 Kratka samoprovjera za poslovanje

- ▶ Leže li osjetljivi dokumenti otvoreno na stolovima ili policama?
- ▶ Jesu li ormari za dokumente, sefovi i podatkovni sefovi jasno dodijeljeni (tko ima pristup čemu)?
- ▶ Postoje li stalne rutine za uništavanje dokumenata (npr. mjesečni "krug brisanja")?
- ▶ Jesu li sigurnosne kopije jasno označene i fizički odvojene od produkcijskih sustava?

Ako je na više točaka odgovor "Da, ali...":

- ▶ Provjeriti strukture, prilagoditi ormare i sefove te definirati jasna pravila za čuvanje, uništavanje i digitalnu sigurnosnu kopiju.
- ▶ Kratka obuka ili podsjetnik za zaposlenike može pomoći razjasniti odgovornosti i pridržavati se postupaka.