kaiserkraft
Mini-ghiduri

Listă de verificare – ce se păstrează unde?

Obiectiv:
Vedeți dintr-o privire ce informații aparțin în dulapul pentru documente, seif sau seif de date, ce trebuie distrus și unde este util și backupul digital.

01 Dulap pentru documente – Pentru documente confidențiale necesare periodic.

Conținuturi tipice:

- [ ] Documente de personal, precum contracte de muncă, evaluări sau concedii medicale – trebuie să fie sigure, dar rapid accesibile.
- [ ] Documente financiare și contabile, precum facturi, bilanțuri sau documente fiscale, care sunt procesate periodic.
- [ ] Contracte în derulare cu clienți, furnizori și parteneri – accesul trebuie reglementat clar.
- [ ] Politici interne, instrucțiuni de operare, siguranță și lucru, pentru ca activitatea zilnică să decurgă fără probleme.

Reguli de bază:

- [ ] Țineți dulapul mereu închis; predați chei sau acces doar persoanelor autorizate.
- [ ] Sortați documentele pe teme și arhivați-le după termenul de păstrare, pentru a evita haosul și timpii de căutare.
- [ ] Transferați regulat documentele expirate în containere protejate pentru distrugerea documentelor, pentru a minimiza riscurile privind protecția datelor.

02 Seif / dulap de securitate – Pentru conținuturi deosebit de valoroase sau critice.

Conținuturi tipice:

- [ ] Documente originale, precum acte de înființare, extrase de carte funciară sau contracte notariale, a căror pierdere ar avea consecințe juridice.
- [ ] Mape de semnături, ștampile de firmă și împuterniciri indispensabile operațional.
- [ ] Suporturi de date cu informații sensibile, precum hard diskuri de backup, stickuri USB sau suporturi de proiect confidențiale.
- [ ] Obiecte de valoare, precum numerar, vouchere sau hardware sensibil (de ex., tokenuri de acces).

Reguli de bază:

- [ ] Ancorați ferm seiful și amplasați-l într-o zonă protejată, discretă, pentru a îngreuna manipulările.
- [ ] Definiți clar drepturile de acces; nu „toți angajații cu cheie”.
- [ ] Documentați accesările, de ex. prin registre de închidere sau liste de acces, pentru a menține responsabilitatea trasabilă.

03 Seif de date / dulap ignifug pentru suporturi de date – Pentru medii sensibile la căldură și umiditate.

Conținuturi tipice:

- ☐ Backupuri ale sistemelor ERP, HR sau de producție, a căror restaurare este critică în caz de urgență.
- ☐ Suporturi de date speciale, precum benzi, SSD-uri sau hard diskuri externe, deosebit de sensibile la căldură și umiditate.
- ☐ Date de proiect arhivate, relevante juridic sau operațional.

Reguli de bază:

- ☐ Utilizați doar dulapuri testate pentru suporturi de date (clase de foc și temperatură adaptate).
- ☐ Rotiți backupurile regulate după o schemă fixă (zilnic, săptămânal, lunar), pentru a evita pierderea datelor.
- ☐ Etichetați clar suporturile de date (conținut, dată, sistem) – pentru restaurare rapidă și imagine de ansam-

04 Ce se distruge? – Folosiți corect distrugătoarele de documente și ștergerea digitală.

Documente pe hârtie:

- ☐ Date cu caracter personal (candidaturi, dosare vechi de personal, liste salariale).
- ☐ Contracte, oferte sau calculații depășite cu informații confidențiale.
- ☐ Printuri cu date de acces, strategii interne sau informații financiare.
- ☐ Note, minute și versiuni intermediare care conțin detalii sensibile.

Reguli de bază:

- ☐ Alegeți nivelul de securitate potrivit nevoii de protecție – niveluri mai ridicate pentru date HR și financiare.
- ☐ Închideți containerele de colectare și goliți-le regulat, pentru a asigura distrugerea completă.

Date digitale:

- ☐ Backupuri depășite, care nu mai sunt necesare.
- ☐ Suporturi de date la sfârșit de viață (hard diskuri defecte, stickuri USB, benzi).
- ☐ Date de test sau copii care conțin conținuturi sensibile.

Sfat: Și digital, drepturile de acces trebuie reglementate clar, iar procesele de ștergere documentate.

05 Combinarea păstrării fizice + backupului digital

Principiu de bază: Informațiile importante sunt păstrate fizic în siguranță și asigurate digital – niciodată duplicate necontrolat.

Exemple:

- **Contracte importante:** Original în dulapul pentru documente sau seif, versiune scanată în arhiva digitală cu trasabilitate de audit.
- **Date critice de operare și instalații:** Versiune de lucru în sistem, backup regulat în seif de date sau seif.
- **Date de personal și HR:** Documente pe hârtie în dulapul pentru documente, dosare digitale în sistem protejat cu managementul drepturilor.

Sfat: Securitatea fizică și digitală se completează – astfel evitați pierderea datelor, furtul sau publicarea accidentală.

06

Scurt autotest pentru activitate

- Documente sensibile sunt lăsate la vedere pe birouri sau rafturi?
- Dulapurile pentru documente, seifurile și seifurile de date sunt alocate clar (cine la ce are acces)?
- Există rutine fixe pentru distrugerea documentelor (de ex., „rundă de ștergere” lunară)?
- Copiile de siguranță sunt etichetate clar și păstrate fizic separat de sistemele productive?

Dacă la mai multe puncte răspunsul este „Da, dar...”:

- Verificați structurile, adaptați soluțiile de dulapuri și seifuri și definiți reguli clare pentru păstrare, distrugere și backup digital.
- O scurtă instruire sau un reminder pentru angajați poate ajuta la clarificarea responsabilităților și respectarea proceselor.