kaiserkraft
Mini guide

Checklist – Cosa va dove?

Obiettivo:
Vedere a colpo d'occhio quali informazioni vanno in armadio documenti, cassaforte o cassaforte per dati, cosa va distrutto e dove è utile anche un backup digitale.

01 Armadio per documenti – Per documenti riservati necessari regolarmente.

Contenuti tipici:

- [ ] Documenti del personale come contratti di lavoro, valutazioni o certificati di malattia – devono essere sicuri, ma rapidamente accessibili.
- [ ] Documenti finanziari e contabili come fatture, bilanci o documenti fiscali che vengono elaborati regolarmente.
- [ ] Contratti in corso con clienti, fornitori e partner – l'accesso deve essere chiaramente regolato.
- [ ] Direttive interne, istruzioni operative, di sicurezza e di lavoro, per garantire una routine fluida.

Regole di base:

- [ ] Tenere sempre chiuso l'armadio; consegnare chiavi o accesso solo a persone autorizzate.
- [ ] Ordinare i documenti per tema e archiviarli in base al periodo di conservazione, per evitare disordine e tempi di ricerca.
- [ ] Trasferire regolarmente i documenti scaduti in contenitori protetti per la distruzione dei documenti, per ridurre i rischi di protezione dei dati.

02 Cassaforte / armadio di sicurezza – Per contenuti particolarmente preziosi o critici.

Contenuti tipici:

- [ ] Documenti originali come atti costitutivi, estratti catastali o contratti notarili, la cui perdita avrebbe conseguenze legali.
- [ ] Cartelle firma, timbri aziendali e procure indispensabili per l'attività.
- [ ] Supporti dati con informazioni sensibili come hard disk di backup, chiavette USB o supporti di progetto riservati.
- [ ] Oggetti di valore come contanti, buoni o hardware sensibile (ad es. token di accesso).

Regole di base:

- [ ] Ancorare saldamente la cassaforte e collocarla in un'area protetta e discreta, per rendere più difficili le manipolazioni.
- [ ] Definire chiaramente i diritti di accesso; non "tutti i collaboratori con chiave".
- [ ] Documentare gli accessi, ad es. con registri di chiusura o liste accessi, per mantenere tracciabili le responsabilità.

03 Cassaforte per dati / armadio ignifugo per supporti dati – Per supporti sensibili a calore e umidità.

Contenuti tipici:

- ☐ Backup di sistemi ERP, HR o di produzione, il cui ripristino è critico in caso di emergenza.
- ☐ Supporti dati speciali come nastri, SSD o hard disk esterni, particolarmente sensibili a calore e umidità.
- ☐ Dati di progetto archiviati, rilevanti sul piano legale o operativo.

Regole di base:

- ☐ Utilizzare solo armadi certificati per supporti dati (classi di fuoco e temperatura adeguate).
- ☐ Ruotare i backup regolari secondo uno schema fisso (giornaliero, settimanale, mensile), per evitare perdite di dati.
- ☐ Etichettare chiaramente i supporti dati (contenuto, data, sistema) – per ripristino rapido e panoramica.

04 Cosa viene distrutto? – Usare correttamente distruggidocumenti ed eliminazione digitale.

Documenti cartacei:

- ☐ Dati personali (candidature, vecchi fascicoli del personale, liste paga).
- ☐ Contratti, offerte o calcoli obsoleti con informazioni riservate.
- ☐ Stampe con dati di accesso, strategie interne o informazioni finanziarie.
- ☐ Note, verbali e versioni intermedie che contengono dettagli sensibili.

Regole di base:

- ☐ Scegliere il livello di sicurezza in base al bisogno di protezione – livelli più alti per dati HR e finanziari.
- ☐ Chiudere i contenitori di raccolta e svuotarli regolarmente, per garantire una distruzione completa.

Dati digitali:

- ☐ Backup obsoleti che non sono più necessari.
- ☐ Supporti dati a fine vita (hard disk difettosi, chiavette USB, nastri).
- ☐ Dati di test o copie che contengono contenuti sensibili.

Suggerimento: Anche in digitale, i diritti di accesso devono essere regolati chiaramente e i processi di

05 Combinare conservazione fisica + backup digitale

Principio di base: Le informazioni importanti sono conservate fisicamente in modo sicuro e salvate in digitale – mai duplicate senza controllo.

Esempi:

- **Contratti importanti:** Originale nell'armadio documenti o in cassaforte, versione scansionata nell'archivio digitale a prova di revisione.
- **Dati operativi e impiantistici critici:** Versione di lavoro nel sistema, backup regolare in cassaforte per dati o cassaforte.
- **Dati del personale e HR:** Documenti cartacei nell'armadio documenti, fascicoli digitali in un sistema protetto con gestione dei diritti.

Suggerimento: Sicurezza fisica e digitale si completano – così si evitano perdita di dati, furto o pubblicazione involontaria.

06

Breve autoverifica per l’azienda

- Documenti sensibili sono lasciati aperti su scrivanie o scaffali?
- Armadi per documenti, casseforti e casseforti per dati sono assegnati chiaramente (chi accede a cosa)?
- Esistono routine fisse per la distruzione dei documenti (ad es. “sessione di eliminazione” mensile)?
- I backup sono etichettati chiaramente e conservati fisicamente separati dai sistemi produttivi?

Se più punti ricevono risposta “Sì, però…”:

- Verificare le strutture, adattare armadi e casseforti e definire regole chiare per conservazione, distruzione e backup digitale.
- Una breve formazione o un promemoria ai collaboratori può aiutare a chiarire le responsabilità e a rispettare le procedure.