kaiserkraft
Miniporadniki

Lista kontrolna – co gdzie należy?

Cel:
Szybko sprawdzić, które informacje trafiają do szafy na dokumenty, sejfu lub sejfu na dane, co należy zniszczyć i gdzie warto dodać kopię cyfrową.

01 Szafa na dokumenty – na poufne dokumenty potrzebne regularnie.

Typowe treści:

- [ ] Dokumenty kadrowe, takie jak umowy o pracę, oceny lub zwolnienia lekarskie – muszą być bezpieczne, ale szybko dostępne.
- [ ] Dokumenty finansowe i księgowe, takie jak faktury, bilanse lub dokumenty podatkowe, które są regularnie przetwarzane.
- [ ] Bieżące umowy z klientami, dostawcami i partnerami – dostęp powinien być jasno uregulowany.
- [ ] Wewnętrzne wytyczne, instrukcje operacyjne, bezpieczeństwa i pracy, aby codzienna praca przebiegała sprawnie.

Podstawowe zasady:

- [ ] Szafę zawsze trzymać zamkniętą; klucz lub dostęp przekazywać tylko osobom uprawnionym.
- [ ] Porządkować dokumenty tematycznie i odkładać je według okresu przechowywania, aby uniknąć chaosu i czasu wyszukiwania.
- [ ] Przeterminowane dokumenty regularnie przenosić do zabezpieczonych pojemników na niszczenie akt, aby minimalizować ryzyka ochrony danych.

02 Sejf / szafa pancerna – na szczególnie wartościowe lub krytyczne treści.

Typowe treści:

- [ ] Oryginały dokumentów, takie jak akty założycielskie, odpisy z ksiąg wieczystych lub umowy notarialne, których utrata miałaby skutki prawne.
- [ ] Teczki do podpisu, pieczęcie firmowe i pełnomocnictwa niezbędne operacyjnie.
- [ ] Nośniki danych z poufnymi informacjami, takie jak dyski kopii zapasowych, pamięci USB lub poufne nośniki projektowe.
- [ ] Przedmioty wartościowe, takie jak gotówka, bony lub wrażliwy sprzęt (np. tokeny dostępu).

Podstawowe zasady:

- [ ] Sejf solidnie zakotwić i ustawić w chronionym, dyskretnym miejscu, aby utrudnić manipulacje.
- [ ] Jasno zdefiniować prawa dostępu; nie „wszyscy pracownicy z kluczem”.
- [ ] Dokumentować dostępy, np. przez protokoły zamknięć lub listy wejść, aby odpowiedzialność była możliwa do prześledzenia.

03 Sejf na dane / szafa ognioodporna na nośniki danych – na media wrażliwe na ciepło i wilgoć.

Typowe treści:

- ☐ Kopie zapasowe systemów ERP, HR lub produkcyjnych, których odtworzenie w sytuacji awaryjnej jest
- ☐ Specjalne nośniki danych, takie jak taśmy, SSD lub dyski zewnętrzne, szczególnie wrażliwe na ciepło i wilgoć.
- ☐ Zarchiwizowane dane projektowe istotne prawnie lub operacyjnie.

Podstawowe zasady:

- ☐ Używać tylko sprawdzonych szaf na nośniki danych (dostosowane klasy ognia i temperatury).
- ☐ Regularnie rotować kopie zapasowe według stałego schematu (dziennie, tygodniowo, miesięcznie), aby uniknąć utraty danych.
- ☐ Jasno opisywać nośniki danych (treść, data, system) – dla szybkiego odtworzenia i przeglądu.

04 Co jest niszczone? – Prawidłowo stosować niszczarki akt i cyfrowe usuwanie.

Dokumenty papierowe:

- ☐ Dane osobowe (aplikacje, stare akta osobowe, listy płac).
- ☐ Nieaktualne umowy, oferty lub kalkulacje z poufnymi informacjami.
- ☐ Wydruki z danymi dostępowymi, strategiami wewnętrznymi lub informacjami finansowymi.
- ☐ Notatki, protokoły i wersje robocze zawierające wrażliwe szczegóły.

Podstawowe zasady:

- ☐ Wybrać poziom bezpieczeństwa odpowiedni do potrzeby ochrony – wyższe poziomy dla danych HR i
- ☐ Zamykać pojemniki zbiorcze i regularnie je opróżniać, aby zapewnić pełne niszczenie.

Dane cyfrowe:

- ☐ Nieaktualne kopie zapasowe, które nie są już potrzebne.
- ☐ Nośniki danych na końcu cyklu życia (uszkodzone dyski, pamięci USB, taśmy).
- ☐ Dane testowe lub kopie zawierające wrażliwe treści.

Wskazówka: Także cyfrowo prawa dostępu powinny być jasno uregulowane, a procesy kasowania

05 Połączyć fizyczne przechowywanie + kopię cyfrową

Podstawowa zasada: Ważne informacje są fizycznie bezpiecznie przechowywane i cyfrowo zabezpieczane – nigdy podwójnie bez kontroli.

Przykłady:

- **Ważne umowy:** Oryginał w szafie na dokumenty lub sejfie, wersja zeskanowana w zgodnym z audytem archiwum cyfrowym.
- **Krytyczne dane operacyjne i instalacyjne:** Wersja robocza w systemie, regularna kopia zapasowa w sejfie na dane lub sejfie.
- **Dane personalne i HR:** Dokumenty papierowe w szafie na dokumenty, akta cyfrowe w chronionym systemie z zarządzaniem uprawnieniami.

Wskazówka: Bezpieczeństwo fizyczne i cyfrowe uzupełniają się – tak unikają Państwo utraty danych, kradzieży lub przypadkowej publikacji.

06

Krótki autotest dla firmy

- Czy poufne dokumenty leżą otwarcie na biurkach lub regałach?
- Czy szafy na dokumenty, sejfy i sejfy na dane są jasno przypisane (kto ma do czego dostęp)?
- Czy istnieją stałe procedury niszczenia akt (np. comiesięczna „runda kasowania”)?
- Czy kopie zapasowe są jasno opisane i przechowywane fizycznie oddzielnie od systemów produkcyjnych?

Jeśli na kilka punktów odpowiedziano „Tak, ale…”:

- Sprawdzić struktury, dostosować szafy i sejfy oraz zdefiniować jasne zasady przechowywania, niszczenia i zabezpieczania cyfrowego.
- Krótkie szkolenie lub przypomnienie dla pracowników może pomóc doprecyzować odpowiedzialności i przestrzegać procedur.