kaiserkraft
Mini-gidsen

# Checklist – Wat hoort waar?

**Doel:**
In één oogopslag zien welke informatie in de documentenkast, kluis of datakluis hoort, wat vernietigd moet worden en waar digitale back-up aanvullend zinvol is.

## 01 Documentenkast – Voor vertrouwelijke documenten die regelmatig nodig zijn.

**Typische inhoud:**

- [ ] Personeelsdocumenten zoals arbeidscontracten, beoordelingen of ziekmeldingen – ze moeten veilig, maar snel toegankelijk zijn.
- [ ] Financiële en boekhoudkundige documenten zoals facturen, balansen of fiscale stukken die regelmatig worden verwerkt.
- [ ] Lopende contracten met klanten, leveranciers en partners – de toegang moet duidelijk geregeld zijn.
- [ ] Interne richtlijnen, bedrijfsinstructies, veiligheids- en werkinstructies, zodat de dagelijkse praktijk soepel loopt.

**Basisregels:**

- [ ] Kast altijd gesloten houden; sleutel of toegang alleen aan bevoegde personen verstrekken.
- [ ] Documenten thematisch sorteren en op bewaartermijn archiveren om chaos en zoektijd te voorkomen.
- [ ] Verlopen documenten regelmatig overbrengen naar beschermde inzamelcontainers voor archiefvernietiging om privacyrisico's te minimaliseren.

## 02 Kluis / waardekast – Voor bijzonder waardevolle of kritieke inhoud.

**Typische inhoud:**

- [ ] Originele documenten zoals oprichtingsstukken, kadastrale uittreksels of notariële contracten waarvan verlies juridische gevolgen zou hebben.
- [ ] Ondertekenmappen, bedrijfsstempels en volmachten die voor de bedrijfsvoering onmisbaar zijn.
- [ ] Gegevensdragers met gevoelige informatie zoals back-upschijven, USB-sticks of vertrouwelijke projectmedia.
- [ ] Waardevolle zaken zoals contant geld, vouchers of gevoelige hardware (bijv. toegangstokens).

**Basisregels:**

- [ ] Kluis stevig verankeren en in een beschermde, onopvallende zone plaatsen om manipulatie te bemoeilijken.
- [ ] Toegangsrechten duidelijk definiëren; niet "alle medewerkers met sleutel".
- [ ] Toegang documenteren, bijv. via sluitprotocollen of toegangslijsten, om verantwoordelijkheid traceerbaar te houden.

## 03 Datakluis / brandwerende kast voor gegevensdragers – Voor media die gevoelig zijn voor hitte en vocht.

**Typische inhoud:**

- ☐ Back-ups van ERP-, HR- of productiesystemen waarvan herstel in noodgevallen kritisch is.
- ☐ Speciale gegevensdragers zoals tapes, SSD's of externe harde schijven die bijzonder gevoelig zijn voor hitte en vocht.
- ☐ Gearchiveerde projectdata die juridisch of operationeel relevant zijn.

**Basisregels:**

- ☐ Gebruik alleen geteste kasten voor gegevensdragers (aangepaste brand- en temperatuurklassen).
- ☐ Regelmatige back-ups volgens vast schema roteren (dagelijks, wekelijks, maandelijks) om gegevensverlies te voorkomen.
- ☐ Gegevensdragers duidelijk labelen (inhoud, datum, systeem) – voor snel herstel en overzicht.

## 04 Wat wordt vernietigd? – Papiervernietigers en digitaal wissen correct inzetten.

**Papieren documenten:**

- ☐ Persoonsgegevens (sollicitaties, oude personeelsdossiers, loonlijsten).
- ☐ Verouderde contracten, offertes of calculaties met vertrouwelijke informatie.
- ☐ Afdrukken met toegangsgegevens, interne strategieën of financiële informatie.
- ☐ Notities, verslagen en tussenstanden die gevoelige details bevatten.

**Basisregels:**

- ☐ Kies het veiligheidsniveau passend bij de beschermingsbehoefte – hogere niveaus voor HR- en financiële
- ☐ Inzamelcontainers afsluiten en regelmatig legen om volledige vernietiging te garanderen.

**Digitale data:**

- ☐ Verouderde back-ups die niet meer nodig zijn.
- ☐ Gegevensdragers aan einde levensduur (defecte harde schijven, USB-sticks, tapes).
- ☐ Testdata of kopieën die gevoelige inhoud bevatten.

**Tip:** Ook digitaal moeten toegangsrechten duidelijk geregeld zijn en wisprocessen worden gedocumenteerd.

## 05 Fysieke opslag + digitale back-up combineren

**Basisprincipe:** Belangrijke informatie wordt fysiek veilig bewaard en digitaal geback-upt – nooit ongecontroleerd dubbel verspreid.

**Voorbeelden:**

- **Belangrijke contracten:** Origineel in de documentenkast of kluis, gescande versie in het revisieveilige digitale archief.
- **Kritieke bedrijfs- en installatiegegevens:** Werkversie in het systeem, regelmatige back-up in datakluis of kluis.
- **Personeels- en HR-data:** Papieren documenten in de documentenkast, digitale dossiers in beschermd systeem met rechtenbeheer.

**Tip:** Fysieke en digitale veiligheid vullen elkaar aan – zo voorkomt u gegevensverlies, diefstal of onbedoelde publicatie.

06

## Korte zelftest voor het bedrijf

- Liggen gevoelige documenten open op bureaus of in stellingen?
- Zijn documentenkasten, kluizen en datakluizen duidelijk toegewezen (wie heeft waar toegang toe)?
- Zijn er vaste routines voor archiefvernietiging (bijv. maandelijkse “wisronde”)?
- Zijn back-ups duidelijk gelabeld en fysiek gescheiden van de productiesystemen opgeslagen?

**Als meerdere punten met “Ja, maar…” worden beantwoord:**

- Structuren controleren, kast- en kluisoplossingen aanpassen en duidelijke regels voor bewaren, vernietigen en digitale back-up vastleggen.
- Een korte training of reminder voor medewerkers kan helpen verantwoordelijkheden te verduidelijken en procedures na te leven.