kaiserkraft
Mini guides

Checklist – What goes where?

Objective:
See at a glance which information belongs in a document cabinet, safe or data safe, what must be destroyed and where digital backup also makes sense.

01 Document cabinet – For confidential documents that are needed regularly.

Typical contents:

- [ ] HR documents such as employment contracts, appraisals or sick notes – they must be secure, yet quickly accessible.
- [ ] Financial and accounting documents such as invoices, balance sheets or tax records that are processed regularly.
- [ ] Current contracts with customers, suppliers and partners – access should be clearly regulated.
- [ ] Internal policies, operating instructions, safety and work instructions to keep daily operations running smoothly.

Basic rules:

- [ ] Always keep the cabinet locked; issue keys or access only to authorised persons.
- [ ] Sort documents by topic and file them by retention period to avoid clutter and time-consuming searches.
- [ ] Regularly move expired documents into secure collection containers for document destruction to minimise data protection risks.

02 Safe / security cabinet – For particularly valuable or critical contents.

Typical contents:

- [ ] Original documents such as incorporation papers, land register extracts or notarised contracts whose loss would have legal consequences.
- [ ] Signature folders, company stamps and powers of attorney that are essential for operations.
- [ ] Data carriers with sensitive information such as backup hard drives, USB sticks or confidential project media.
- [ ] Valuables such as cash, vouchers or sensitive hardware (e.g. access tokens).

Basic rules:

- [ ] Anchor the safe firmly and place it in a protected, discreet area to make tampering more difficult.
- [ ] Clearly define access rights; not “all employees with a key”.
- [ ] Document access, e.g. via lock logs or access lists, to keep responsibilities traceable.

03 Data safe / fireproof cabinet for data carriers – For media sensitive to heat and moisture.

Typical contents:

- ☐ Backups of ERP, HR or production systems whose recovery is critical in an emergency.
- ☐ Special data carriers such as tapes, SSDs or external hard drives that are especially sensitive to heat and moisture.
- ☐ Archived project data that is legally or operationally relevant.

Basic rules:

- ☐ Use only tested cabinets for data carriers (adapted fire and temperature classes).
- ☐ Rotate regular backups according to a fixed schedule (daily, weekly, monthly) to avoid data loss.
- ☐ Clearly label data carriers (content, date, system) – for quick recovery and overview.

04 What gets destroyed? – Use document shredders and digital deletion correctly.

Paper documents:

- ☐ Personal data (applications, old personnel files, payroll lists).
- ☐ Outdated contracts, offers or calculations with confidential information.
- ☐ Printouts with login details, internal strategies or financial information.
- ☐ Notes, minutes and interim versions containing sensitive details.

Basic rules:

- ☐ Choose the security level to match the protection need – higher levels for HR and financial data.
- ☐ Lock collection containers and empty them regularly to ensure complete destruction.

Digital data:

- ☐ Outdated backups that are no longer needed.
- ☐ End-of-life data carriers (defective hard drives, USB sticks, tapes).
- ☐ Test data or copies containing sensitive content.

Tip: Access rights should also be clearly regulated digitally, and deletion processes documented.

05 Combine physical storage + digital backup

Basic principle: Important information is stored securely in physical form and backed up digitally – never duplicated without control.

Examples:

- **Important contracts:** Original in the document cabinet or safe, scanned version in the audit-proof digital archive.
- **Critical operational and plant data:** Working version in the system, regular backup in a data safe or safe.
- **Personnel and HR data:** Paper documents in the document cabinet, digital files in a protected system with rights management.

Tip: Physical and digital security complement each other – helping you avoid data loss, theft or accidental publication.

06

Short self-check for operations

- Are sensitive documents left openly on desks or shelves?
- Are document cabinets, safes and data safes clearly assigned (who has access to what)?
- Are there fixed routines for document destruction (e.g. a monthly “deletion round”)?
- Are backups clearly labelled and stored physically apart from production systems?

If several points are answered with “Yes, but…”:

- Review structures, adapt cabinet and safe solutions and define clear rules for storage, destruction and digital backup.
- A short training session or reminder for employees can help clarify responsibilities and follow procedures.