kaiserkraft
Mini útmutatók

Ellenőrzőlista – mi hová kerül?

Cél:
Egy pillantással látható, mely információ kerül iratszekrénybe, széfbe vagy adatszéfbe, mit kell megsemmisíteni, és hol hasznos a digitális mentés.

01 Iratszekrény – Rendszeresen szükséges bizalmas dokumentumokhoz.

Tipikus tartalmak:

- [ ] Személyzeti dokumentumok, például munkaszerződések, értékelések vagy betegállomány-igazolások – biztonságban kell lenniük, de gyorsan elérhetőnek is.
- [ ] Pénzügyi és könyvelési dokumentumok, például számlák, mérlegek vagy adóiratok, amelyeket rendszeresen feldolgoznak.
- [ ] Folyamatban lévő szerződések ügyfelekkel, beszállítókkal és partnerekkel – a hozzáférést világosan
- [ ] Belső irányelvek, üzemeltetési, biztonsági és munkautasítások, hogy a napi működés zökkenőmentes legyen.

Alapszabályok:

- [ ] A szekrényt mindig zárva kell tartani; kulcsot vagy hozzáférést csak jogosult személyek kapjanak.
- [ ] A dokumentumokat téma szerint rendezni és megőrzési idő alapján iktatni, hogy elkerülhető legyen a káosz és a hosszú keresés.
- [ ] A lejárt dokumentumokat rendszeresen védett iratmegsemmisítő gyűjtőedénybe kell helyezni, hogy csökkenjenek az adatvédelmi kockázatok.

02 Széf / értékbiztonsági szekrény – Különösen értékes vagy kritikus tartalmakhoz.

Tipikus tartalmak:

- [ ] Eredeti okiratok, például alapító dokumentumok, tulajdoni lapok vagy közjegyzői szerződések, amelyek elvesztése jogi következményekkel járna.
- [ ] Aláírási mappák, céges bélyegzők és meghatalmazások, amelyek a működéshez nélkülözhetetlenek.
- [ ] Érzékeny információkat tartalmazó adathordozók, például mentési merevlemezek, USB-kulcsok vagy bizalmas projektmédiumok.
- [ ] Értékek, például készpénz, utalványok vagy érzékeny hardver (pl. hozzáférési tokenek).

Alapszabályok:

- [ ] A széfet szilárdan rögzíteni és védett, feltűnésmentes helyre tenni, hogy nehezebb legyen manipulálni.
- [ ] A hozzáférési jogokat világosan meghatározni; ne „minden kulccsal rendelkező munkatárs”.
- [ ] A hozzáféréseket dokumentálni, pl. zárási naplókkal vagy belépési listákkal, hogy a felelősség követhető maradjon.

03 Adatszéf / tűzvédelmi szekrény adathordozókhoz – Hőre és nedvességre érzékeny médiumokhoz.

Tipikus tartalmak:

- ☐ ERP-, HR- vagy termelési rendszerek biztonsági mentései, amelyek helyreállítása vészhelyzetben kritikus.
- ☐ Speciális adathordozók, például szalagok, SSD-k vagy külső merevlemezek, amelyek különösen érzékenyek hőre és nedvességre.
- ☐ Archivált projektadatok, amelyek jogilag vagy működésileg relevánsak.

Alapszabályok:

- ☐ Csak bevizsgált adathordozó-szekrényeket használni (megfelelő tűz- és hőmérsékleti osztályokkal).
- ☐ A rendszeres mentéseket fix séma szerint rotálni (napi, heti, havi), hogy elkerülhető legyen az adatvesztés.
- ☐ Az adathordozókat világosan felcímkézni (tartalom, dátum, rendszer) – gyors helyreállításhoz és áttekin-

04 Mit kell megsemmisíteni? – Iratmegsemmisítő és digitális törlés helyes használata.

Papíralapú dokumentumok:

- ☐ Személyes adatok (pályázatok, régi személyi akták, bérlisták).
- ☐ Elavult szerződések, ajánlatok vagy kalkulációk bizalmas információkkal.
- ☐ Kinyomtatott hozzáférési adatok, belső stratégiák vagy pénzügyi információk.
- ☐ Jegyzetek, jegyzőkönyvek és köztes verziók, amelyek érzékeny részleteket tartalmaznak.

Alapszabályok:

- ☐ A biztonsági szintet a védelmi igényhez igazítani – magasabb szintek HR- és pénzügyi adatokhoz.
- ☐ A gyűjtőedényeket lezárni és rendszeresen üríteni, hogy a teljes megsemmisítés biztosított legyen.

Digitális adatok:

- ☐ Elavult biztonsági mentések, amelyekre már nincs szükség.
- ☐ Élettartamuk végén lévő adathordozók (hibás merevlemezek, USB-kulcsok, szalagok).
- ☐ Tesztadatok vagy másolatok, amelyek érzékeny tartalmat hordoznak.

Tipp: Digitálisan is világosan kell szabályozni a hozzáférési jogokat, és dokumentálni a törlési folyamatokat.

05 Fizikai megőrzés + digitális mentés kombinálása

Alapelv: A fontos információkat fizikailag biztonságosan tárolják és digitálisan mentik – soha nem duplázzák ellenőrizetlenül.

Példák:

- **Fontos szerződések:** Eredeti az iratszekrényben vagy széfben, szkennelt verzió az auditbiztos digitális archívumban.
- **Kritikus üzemi és berendezésadatok:** Munkaverzió a rendszerben, rendszeres mentés adatszéfben vagy széfben.
- **Személyzeti és HR-adatok:** Papíralapú dokumentumok az iratszekrényben, digitális akták védett rendszerben jogosultságkezeléssel.

Tipp: A fizikai és digitális biztonság kiegészíti egymást – így elkerülhető az adatvesztés, a lopás vagy a véletlen közzététel.

06

Rövid önellenőrzés az üzem számára

- Érzékeny dokumentumok nyíltan hevernek az asztalokon vagy polcokon?
- Az iratszekrények, páncélszekrények és adatszéfek egyértelműen ki vannak osztva (ki mihez fér hozzá)?
- Vannak rögzített rutinok az iratmegsemmisítésre (pl. havi „törlési kör”)?
- A biztonsági mentések egyértelműen címkézettek és fizikailag elkülönítve vannak a termelési rendszerektől?

Ha több pontra „Igen, de…” a válasz:

- Ellenőrizni a struktúrákat, igazítani a szekrény- és széfmegoldásokat, és világos szabályokat rögzíteni a megőrzésre, megsemmisítésre és digitális mentésre.
- Egy rövid képzés vagy emlékeztető a munkatársaknak segíthet tisztázni a felelősségeket és betartani a folyamatokat.