Tipplap az adatbiztonságról az operatív adatkezelésben
2022. április

Ezen tipplap fordítását a CartONG segítette a CLEAR Global és a francia Európai Ügyek és Külügyek Minisztériuma támogatásának köszönhetően.

Bevezetés
Az adatbiztonság az adatfelelősség kulcsfontosságú eleme: az operatív reagáláshoz szükséges adatok biztonságos, etikus és hatékony kezelése. Olyan fizikai, technológiai és eljárási intézkedéseket foglal magában, amelyek védik az adatok titkosságát, integritását és elérhetőségét, és megakadályozzák azok véletlen vagy szándékos, jogellenes vagy más módon jogosulatlan elvesztését, megsemmisítését, megváltoztatását, megszerzését vagy nyilvánosságra hozatalát.

Ez a tipplap egy sor ajánlott intézkedést kínál az operatív adatkezelés adatbiztonsága érdekében. Az intézkedéseket a vonatkozó intézményi megbízatásokkal, irányelvekkel, valamint a jogi és szabályozási keretekkel összhangban kell végrehajtani.

Megfelelő jelszókezelés alkalmazása
- Biztosítsa eszközeit és fiókjait erős jelszavakkal, amelyek számokat, nagybetűket és kisbetűket, valamint legalább 16 karaktert egyaránt tartalmaznak jelszavanként.
- Engedélyezze a többlépcsős azonosítást minden fiókhoz.
- Ne használja ugyanazt a jelszót több fiókhoz.
- Ne tároljon jelszavakat fizikailag (pl. jegyzetpapíron) vagy digitálisan (egy fájlban az eszközén) és ne ossza meg a jelszavát másokkal.
- Ne engedélyezze az 'Emlékezzen rám' funkciót az alkalmazásokban és böngészőkben.
- Készüléke elvesztése vagy eltulajdonítása esetén azonnal cserélje le online fiókjainak jelszavait.

Használjon antivírus/anti-malware szoftvert
- Győződjön meg róla, hogy a megfelelő antivírus/anti-malware szoftverrel rendelkeznek a készülékei.
- Ha kérdése merül fel a megfelelő eszközökkel vagy azok konfigurációjával kapcsolatban, forduljon az irodájában dolgozó informatikai szakemberhez.

Tartsa naprakészen a szoftvereket és az operációs rendszereket.
- Rendszeresen ellenőrizze, hogy készüléke és az azon lévő szoftverek, alkalmazások és böngészőbővítmények naprakészek, és engedélyezze az operációs rendszerek automatikus frissítését.
- Használjon olyan böngészőket, mint a Chrome vagy a Firefox, amelyek automatikus biztonsági frissítéseket kapnak.
- A nap végén állítsa le készülékeit, hogy lehetővé tegye a frissítéseket, és hogy védelmet nyújtson a támadások ellen.

Kerülje el az adathalász csalásokat, és ügyeljen arra, hogy mire kattint
- Ha gyanús e-mailt vagy üzenet kap, mindig ellenőrizze a feladó címét/elérhetőségét, és csak akkor kattintson a linkekre vagy mellékletekre, ha megbízik a feladóban.
- Ne válaszoljon gyanús e-mailekre, és ne továbbítsa azokat kollégáinak.
- Minden gyanús tevékenységet jelentsen az informatikai támogatást nyújtó csapatának.

Használja a mobileszközöket felelősséggel

- **Amennyiben lehetséges, munkavégzéshez használjon külön eszközöket. A munkához használt eszközöket mindig tartsa biztonságos helyen, és feleslegesen ne hordozza őket.**
- **Csak olyan, szervezetileg jóváhagyott üzenetküldő eszközt használjon, amely biztosítja a végpontok közötti titkosítást.**
- **Minimalizálja, és amikor csak lehetséges, kapcsolja ki a Bluetooth-kapcsolatot.**
- **Amikor online dolgozik, használjon a munkahelye által jóváhagyott virtuális magánhálózatot (VPN). Mindig jelentkezzen ki a fiókjaiból, amikor közösségi számítógépet vagy eszközt használ.**
- **Tiltsa le a biometrikus feloldó funkciókat - különösen helyváltoztatás közben.**

Védje az érzékeny adatokat és alkalmazzon adatminimalizálást

- **Tartson fenn egy adateszköz-nyilvántartást, amely jelzi az irodája által kezelt egyes adattípusok érzékenységi szintjét. Rendszeresen ellenőrizze az érzékenységi szinteket a kontextus változásának megfelelően.**
- **Csak az adott adatkezelési tevékenység rendeltetésének és céljainak eléréséhez szükséges minimális adatmennyiséget gyűjtse.**
- **Az érzékeny adatokat csak addig őrizze meg, amíg az az adatkezelés céljának teljesítéséhez szükséges, valamint amíg az alkalmazandó iránymutatások, törvények és rendeletek megkövetelik.**
- **Csak a szervezete által jóváhagyott eszközök és csatornák segítségével továbbítson vagy tároljon adatokat (helyileg egy vállalati szerveren, számítógépen vagy laptopon; vagy távirányítású szervereken és rendszereken, olyan alkalmazásokon keresztül, mint a OneDrive, a SharePoint és a Teams).**
- **Védje jelszóval az érzékeny adatokat tartalmazó fájlokat (Word, Excel, PDF), és külön csatornákon ossza meg ezeket a különböző dokumentumokhoz tartozó jelszavakat (pl. SMS-ben küldje a jelszót egy e-mailben elküldött dokumentumhoz).**
- **Korlátozza és gondosan ellenőrizze az érzékeny adatokhoz hozzáférő személyek számát.**
- Határozza meg az összes kezelt adat megőrzésének és megsemmisítésének ütemtervét, és használjon megfelelő eszközöket az adatok megsemmisítésére.
- Titkosítsa e-mail üzeneteit.

Kiemelt források

- IASC Operatív útmutató az adatok felelősségéről a humanitárius tevékenységek során
- Útmutató az adatesemények kezeléséhez
- Tipplap az online konferencia-eszközök felelősségteljes használatáról

A humanitárius műveletek során előkerülő érzékeny adatok kezelésével kapcsolatos további információkért látogasson el a Központ weboldalának Adatfelelősség *oldalára, vagy vegye fel a kapcsolatot csapatunkkal a centrehumdata@un.org címen.*