

Narábanie s dokumentmi označenými „NATO UNCLASSIFIED“

Pri zaobchádzaní s dokumentmi označenými ako „NATO UNCLASSIFIED“ (ďalej len „NU“) je potrebné dodržiavať minimálne bezpečnostné požiadavky týkajúce sa narábania s týmto druhom informácií NATO. Aj napriek tomu, že nejde o utajované informácie, označenie „NU“ je bezpečnostným označením NATO. Takto označené informácie NATO si vyžadujú určitý stupeň ochrany. Bezpečnostné štandardy, ktoré je potrebné aplikovať počas narábania s NU informáciami uvádzame nižšie.

Je dôležité zdôrazniť, že NU informácia môže byť použitá len na oficiálne účely. Prístup k NU informácii môžu mať len osoby, orgány alebo organizácie za účelom plnenia oficiálnych cieľov NATO.

Minimálne bezpečnostné požiadavky na ochranu NU informácií:

1. „hard copy“ NU informácia (papierová podoba)
 - a) ukladanie: NU informácia musí byť uschovaná tak, aby ste adekvátne zabránili neoprávnenému prístupu k nej,
 - b) fyzický prenos: môže sa prenášať zabalená v jednej nepriehľadnej obálke a môže byť prepravovaná bežnou poštovou službou,
 - c) ničenie: môže byť zničená akýmkoľvek prostriedkami, ktoré ju zničia takým spôsobom, aby nebolo možné jej opätovné zrekonštruovanie alebo prečítanie.
2. elektronická NU informácia
Ak je NU informácia spracovávaná, uchovávaná alebo prenášaná prostredníctvom elektromagnetického systému musí byť zabezpečená jej integrita, dôvernosť a dostupnosť.
 - a) ochrana dôvernosti NU – zabezpečiť, aby informácia nebola dostupná alebo odhalená pred neoprávnenou osobou, entitou,
 - b) ochrana integrity NU – zabezpečiť, aby informácia nebola pozmenená alebo zničená neoprávneným spôsobom,
 - c) zabezpečenie dostupnosti NU- zabezpečiť, aby bola informácia dostupná v jej hmotnej podobe kedykoľvek, ak o to požiada oprávnená osoba alebo entita.

Rovnako je potrebné zabezpečiť aj samotné podporné systémové služby a zdroje, v rámci ktorých sa s NU informáciouarába.

- a) musí sa zabezpečiť spôsob ako spoľahlivo identifikovať a overiť osoby, ktoré sú oprávnené k prístupu k NU informácii,
- b) musí sa zaviesť kontrolný mechanizmus, ktorý bude sledovať oprávnené prístupy, ktoré budú mať len osoby na základe princípu „need to know“,
- c) musí sa zaviesť kontrolný systém, ktorý bude kontrolovať prepojenie na systémy, v ktorých saarába s NU informáciou.

Princíp „Need-to-know“ – princíp, na základe ktorého je jasne stanovené, že eventuálny príjemca informácie má právo na prístup k tejto informácii a jej držba je pre príjemcu potrebná za účelom plnenia jeho oficiálnych úloh alebo služieb.