

---

# FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ PROSTREDIA: ZÁKLADY



Financované  
Európskou úniou  
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ  
CENTRUM  
KYBERNETICKEJ  
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ  
UNIVERZITA V BRATISLAVE

## Definícia

Fyzická bezpečnosť je súbor opatrení a prostriedkov navrhnutých na ochranu osôb a hmotného i nehmotného majetku pred fyzickými hrozbami.

### Primárne ciele:

- Zabrániť neoprávnenému fyzickému prístupu
- Ochrana pred krádežou a poškodením
- Prevencia sabotáže a vandalizmu
- Ochrana života a zdravia ľudí

### Význam:

- Ochrana citlivých informácií
- Zabezpečenie neprerušenej prevádzky
- Budovanie dôvery klientov
- Splnenie legislatívnych požiadaviek

## Zameranie

Ochrana technickej infraštruktúry pred hrozbami plynúcimi z okolitého prostredia.

### Environmentálne hrozby:

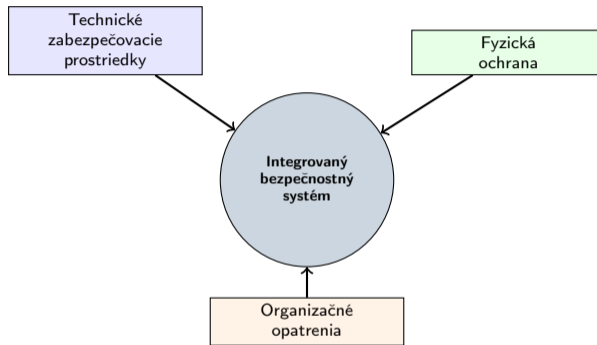
- Požiar
- Voda (zatopenie, vlhkosť)
- Výpadky elektriny
- Extrémne teploty
- Prach a znečistenie

### Koncept environmentálnej bezpečnosti:

- Priemyselné havárie
- Nedostatok prírodných zdrojov
- Klimatické zmeny
- Nekontrolovaná ťažba surovín

## Dôležité

Fyzická bezpečnosť a bezpečnosť prostredia sú neoddeliteľne spojené



## Kľúčová myšlienka

Účinnú ochranu dosiahneme len kombináciou všetkých troch subsystémov

## 1. Mechanické zábranné prostriedky (MZP):

- Oplotenie, brány, turnikety
- Bezpečnostné dvere a okná
- Mreže, rolety
- Trezory a úschovné zariadenia

## 2. Poplachové systémy (PS):

- Elektrické zabezpečovacie systémy (EZS)
- CCTV kamery
- Systémy kontroly vstupu
- Požiarna signalizácia

## 3. Ostatné zariadenia:

- Detektory látok a predmetov
- Zariadenia proti odpočúvaniu
- Skartovače a ničiče nosičov

### Cieľ MZP

Vytvoriť **časové oneskorenie** medzi okamihom napadnutia a dokončením napadnutia.

## 1. Obvodová (perimetrická) ochrana

Plot, brány, bariéry, IR senzory

## 2. Plášťová ochrana

Dvere, okná, steny

## 3. Priestorová

Pohybové detektory

## 4. Predmetová

Trezor, počítač

## Formy fyzickej ochrany:

- Strážna služba
- Bezpečnostný dohľad
- Ochranný sprievod
- Kontrolná priepustková služba
- Bezpečnostný výjazd (zásahové jednotky)

## Z hľadiska časového:

- Viazaná na pracovnú dobu
- Nepretržitá (24/7)
- Nárazová (podľa potreby)

## Z hľadiska rozsahu:

- Priepustková (vrátnici)
- Obvodová (po perimetri)
- Celoplošná (pochôdzky)
- Sprevádzajúca
- Prehľadná dozorová (CCTV)
- Zásahová

## Kľúčová úloha

Bezpečnostný dohľad, kontrola dodržiavania opatrení a **aktívny zákrok** pri narušení.

## Definícia

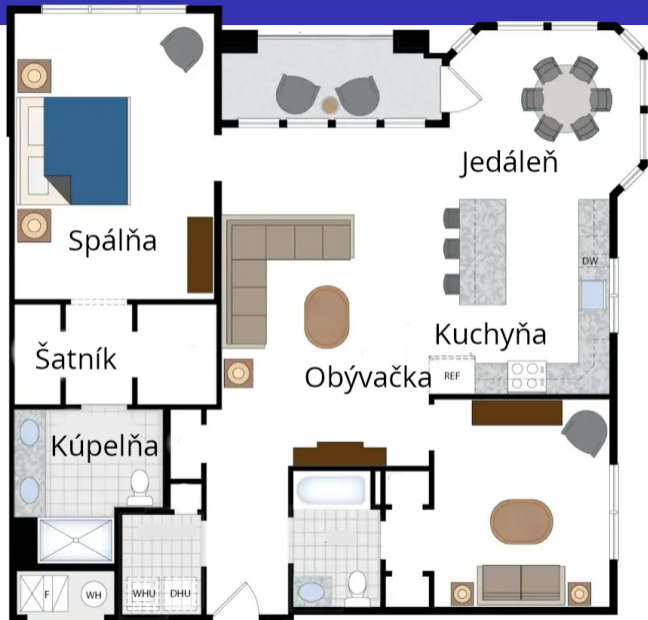
Súhrn administratívno-normatívnych a režimových opatrení - systém poriadku a režimu.

### Hlavné oblasti úpravy:

- 1 **Vstupný a výstupný režim** - kto smie kam a kedy vstúpiť
- 2 **Materiálny a expedičný režim** - kontrola pohybu materiálu a zásielok
- 3 **Prevádzkový režim** - pravidlá počas prevádzky
- 4 **Kľúčový poriadok** - správa kľúčov a prístupových kariet

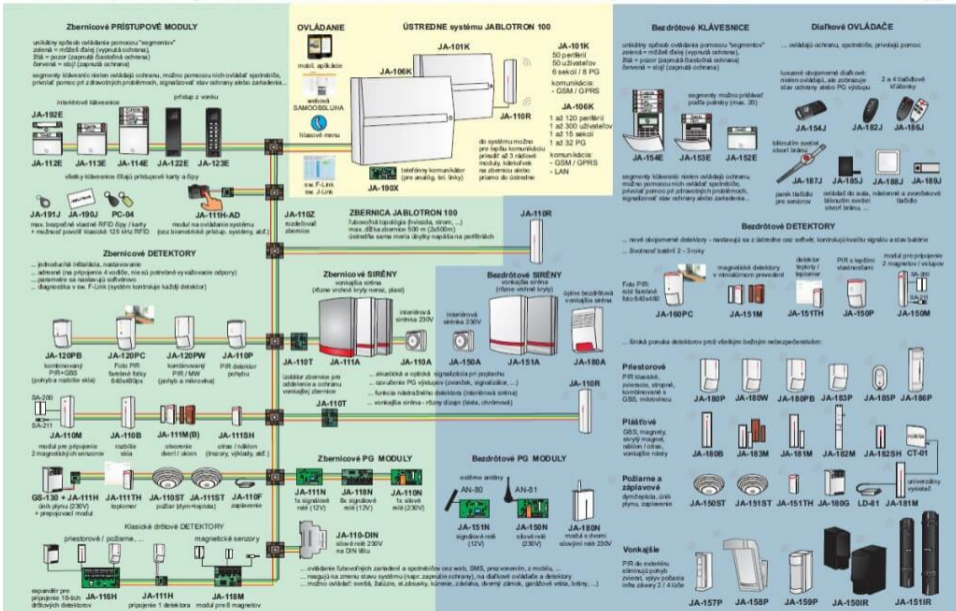
### Forma:

- Interné smernice, pokyny, nariadenia, plány
- Vychádzajú z právnych predpisov (GDPR, zákon o utajovaných skutočnostiach, požiarne ochrana, atď.)



# Prehľad prvkov systému JABLOTRON 100. Alarm s revolučným ovládaním.

www.jablotron.sk





GSM telefon



GSM telefon



telefon -pevná linka



tlačítkové tlačítko



CCTV s WEB serverem



rádiová vysílací stanice



síť GSM



síť pevné linky - ISDN



rádiové pokrytí  
kmitočtové pásmo 420-470 MHz



Pult centralizované ochrany - PCO



příjezd hasičského vozu nebo rychlé záchranné služby



okamžitý zásah bezpečnostní agentury

## Kľúčové zistenie

Hranice medzi fyzickou a kybernetickou bezpečnosťou sa čoraz viac stierajú a stávajú sa vzájomne závislými.

### Fyzický prístup = Digitálny kompromis:

- Priama inštalácia malvéru/spyvéru
- Strata alebo krádež zariadení
- Neoprávnené kopírovanie dát
- Obchádzanie firewallov

### Štatistiky:

- 88% lídrov zaznamenalo nárast fyzických hrozieb (2022)
- 83% uviedlo negatívny dopad na kontinuitu prevádzky
- Fyzické narušenia často predchádzajú únikom dát

## Príklad

Ukradnutý notebook s citlivými dátami = kybernetický incident

## Regulácie

GDPR, NIS2, CCPA/CPRA vyžadujú fyzickú ochranu dát

## Tri zlaté pravidlá:

### 1. ZAMYKANIE

- Vždy zamknite obrazovku (Win+L, Cmd+Ctrl+Q)
- Auto-lock po 15 min
- Silné PIN/heslá
- Biometria (Face ID, odtlačky)

### 2. DOHĽAD

- Nikdy nenechávajte zariadenia bez dozoru
- Pozor na "shoulder surfing"
- Používajte privacy filtre
- Majte zariadenia pri sebe

### 3. ZÁLOHOVANIE

- Pravidelné zálohy
- Šifrovanie disku
- "Nájst' moje zariadenie"
- Plán pre prípad straty

## Pred cestou:

- Minimalizujte počet zariadení
- Nainštalujte aktualizácie
- Zapnite zámky a MFA
- Skontrolujte nastavenia súkromia
- Zakážte sledovanie polohy

## Počas cestovania:

- NIKDY verejné Wi-Fi bez VPN
- Vypnite Wi-Fi a Bluetooth, keď nepoužívate
- Pozor na USB porty (juice jacking)
- Nepoužívajte verejné počítače

## NIKDY!

- Nepripájajte neznáme USB/nabíjačky
- Nenechávajte zariadenia v aute
- Neprihlasujte sa na verejných PC
- Nedôverujte verejným Wi-Fi

## Tip

Používajte vlastnú nabíjačku a powerbanku. VPN je povinnosť, nie luxus

## ITAD - IT Asset Disposition

Proces bezpečného vyradovania IT zariadení z prevádzky.

### Pre zariadenia s neodstrániteľnými diskami:

- Mobilné telefóny, tablety
- Inteligentné hodinky
- **CELÉ zariadenie na zničenie**
- Certifikát o zničení

### Pre počítače:

- Odstránenie šifrovaného HDD
- Bezpečné uloženie alebo zničenie
- Fyzické zničenie (vrtanie, drvenie)

### NIKDY!

- Nevhadzujte disky do koša
- Formátovanie NESTAČÍ
- Nevkladajte nájsené USB do PC
- Nepredávajte bez vymazania

### Prečo?

Špecializovaný softvér dokáže obnoviť dáta z "vymazaného" disku

## Fyzické zabezpečenie:

- Káblové zámky (Kensington)
- Uzamykateľné zásuvky/skrinky
- Skladovanie mimo dohľadu
- Nikdy nenechávať na viditeľných miestach

## Softvérové opatrenia:

- Manuálne zamykanie (Win+L)
- Auto-lock po 15 min (max)
- Šifrovanie disku
- Vzdialené vymazanie

## Stratená prístupová karta?

### OKAMŽITE NAHLÁSIŤ!

- 1 Bezpečnostnému oddeleniu
- 2 IT oddeleniu
- 3 Priamemu nadriadenému

Karta bude zablokovaná v systéme.

## Riziko

Neohlásená stratená karta = otvorené dvere

## Citlivé oblasti vyžadujú dodatočnú ochranu:

- Serverové miestnosti a dátové centrá
- Kancelárie vedenia
- Vývojové a výskumné laboratóriá
- IT a sieťové administrátorské pracoviská

## Technológie kontroly prístupu:

- Biometrické skenery
- RFID karty a kľúčenky
- Sledovanie pohybu (kto, kde, kedy)
- Turnikety proti tailgatingu
- Video surveillance (CCTV)

## Organizačné opatrenia:

- Jasná politika prístupu
- Definícia oprávnení
- Školenie zamestnancov
- Pravidelné preverovanie oprávnení
- Okamžité odoberanie pri zmene pozície

## Princíp najmenších oprávnení

Prístup len tam, kde je to nevyhnutne potrebné pre výkon práce.

## Čo je ITAM?

Proces, ktorý zabezpečuje, že IT aktíva sú zaúčtované, nasadené, udržiavané, aktualizované a zlikvidované v správnom čase.

### Prečo je ITAM dôležitý?

- 1 **Jeden zdroj pravdy** - komplexný prehľad o aktívach
- 2 **Úspora nákladov** - eliminuje zbytočné nákupy
- 3 **Bezpečnosť** - sledovanie neoprávneného HW
- 4 **Compliance** - dodržanie licencií a predpisov

### Proces ITAM:

- 1 Inventarizácia aktív (čo, kde, kedy, koľko)
- 2 Výpočet nákladov životného cyklu
- 3 Sledovanie (záruky, licencie, zmluvy)
- 4 Údržba a aktualizácie
- 5 Finančné plánovanie

## Bezpečnostný aspekt

ITAM identifikuje neoprávnený hardvér, ktorý môže zaviesť malvér alebo uľahčiť úniky dát

## Tri strategické dôvody:

- 1 **Ochrana pred rizikami**
  - Likvidačné finančné sankcie
  - Súdne spory
  - Strata licencií
- 2 **Udržanie dôvery**
  - Dôvera zákazníkov
  - Reputácia na trhu
  - Konkurenčná výhoda
- 3 **Prevádzková kontinuita**
  - Prevencia útokov
  - Rýchla obnova
  - Odolnosť systémov

## Kľúčové regulácie:

- **GDPR** - Ochrana osobných údajov
- **NIS2** - Kybernetická bezpečnosť
- **ISO 27001** - ISMS
- **SOC 2** - Systémové kontroly
- **PCI DSS** - Platobné karty
- **HIPAA** - Zdravotné dáta
- **SOX** - Finančné reportovanie

### GDPR pokuta

Až 20 mil. € alebo 4% globálneho obratu (podľa toho, čo je vyššie)

Vaše pravidlo	Kybernetická bezpečnosť	Normy a zákony
Minimalizácia dát	Znižuje útočnú plochu. Čo neexistuje, nemôže byť ukradnuté.	GDPR, Článok 5(1)(c): Minimalizácia údajov
Klasifikácia dát	Zabraňuje únikom. Silnejšia ochrana citlivých dát.	ISO 27001, A.5.12: Klasifikácia informácií
Silné heslá + MFA	Obrana proti brute-force, credential stuffing, account takeover	GDPR, Článok 32; ISO 27001, A.5.17
Politika čistého stola	Znižuje insider threat, shoulder surfing, krádež údajov	ISO 27001, A.7.7: Clean Desk & Clear Screen
Hlásenie incidentov	Spúšťa Incident Response, zabraňuje šíreniu útokov	GDPR, Článok 33: 72-hod. lehota; ISO 27001, A.16

## Kľúčová myšlienka

Každé bezpečnostné pravidlo má dvojaké opodstatnenie: **ochrana pred hrozbami a splnenie zákonných požiadaviek.**

## Clean Desk - Čistý stôl:

- Žiadne citlivé dokumenty na stole
- Žiadne USB kľúče, notebooky bez dozoru
- Žiadne poznámky s heslami
- Žiadne vizitky návštevníkov

## Clear Screen - Prázdna obrazovka:

- Vždy zamknúť pri odchode (aj na 1 min)
- Win+L (Windows), Cmd+Ctrl+Q (Mac)
- Auto-lock max 15 min
- Žiadne heslá na lístkoch na monitore

## Prečo je to dôležité?

- Externí dodávatelia v priestoroch
- Upratovací personál
- Návštevy
- Nespokojní kolegovia
- Odpozorovanie (shoulder surfing)

## Príklad

Heslo na lístku na monitore = kľúč od celej firmy pre každého, kto prejde okolo

## Praktické kroky

Pri odchode: zamknúť PC + uzamknúť dokumenty do zásuvky

## Čo je Shoulder Surfing?

Technika sociálneho inžinierstva - sledovanie citlivých informácií pohľadom cez rameno.

### Čo môže útočník získať?

- Heslá a PIN kódy
- Jednorazové 2FA kódy
- Obsah e-mailov a dokumentov
- Čísla bankových účtov
- Strategické firemné informácie

### Rizikové miesta:

- Open-space kancelárie
- Verejná doprava
- Kaviarne, letiská
- Bankomaty

### Obranné opatrenia:

- 1 **Všímavosť** - sledujte okolie
- 2 **Privacy filtre** - zužujú pozorovací uhol
- 3 **Strategická poloha** - chrbát k stene
- 4 **Zakrývanie klávesnice** - pri PIN kódoch
- 5 **Zníženie jasů** - sťažuje čítanie z diaľky

### Privacy Screen

Osoba z boku vidí čiernu obrazovku, vy máte jasný obraz

## Problém

Bežné metódy likvidácie sú **NEDOSTATOČNÉ**: vyhodenie do koša, formátovanie disku

### Papierové dokumenty:

- **Skartovačka** s krížovým rezom (cross-cut)
- Nie pozdĺžny rez (ľahko zložitelné)
- Politika "Shred-all" - skartovať všetko
- Eliminuje ľudskú chybu pri rozhodovaní

### Hrozba: Dumpster Diving

- Prehrabávanie v odpadkoch
- Získanie citlivých dokumentov
- Rekonštrukcia skartovaných papierov

### Elektronické médiá:

- HDD, USB, CD/DVD, záložné pásky
- Fyzické zničenie (vrtanie, drvenie)
- Priemyselná skartovačka na elektroniku
- **NESTAČÍ**: formátovanie, delete

### Certifikát o zničení

Pri likvidácii väčšieho objemu použite certifikovanú firmu.

- Profesionálna likvidácia
- Právny dôkaz pre GDPR audit

## Prístupová karta = fyzický kľúč k firemným aktívam

Zaobchádzajte s ňou ako s kľúčmi od vlastného domu

### Základné pravidlá:

- 1 **Osobná zodpovednosť** - neprenosná
- 2 **Nikdy nepožičiavať** kolegom ani iným
- 3 **Viditeľné nosenie** v priestoroch
- 4 **Okamžité hlásenie** straty/krádeže
- 5 **Individuálne použitie** - vlastné karty

### Prečo je to dôležité?

- Audit - systém vie, kto kde bol
- Zodpovednosť - pri incidente
- Prevencia - zabránenie neoprávnenému vstupu
- Bezpečnosť - ochrana citlivých oblastí

### Stratená karta

Okamžite nahlásiť → zablokovanie v systéme → prevencia zneužitia

### Príklad

Zamestnanec požičal kartu kamarátovi, aby sa dostal do budovy. Kamarát ukradol notebooky. Kto je zodpovedný?  
**Zamestnanec!**

## Čo je Tailgating?

Neoprávnená osoba prejde cez zabezpečený vchod tesne za oprávnenou osobou, ktorá jej vedome alebo nevedome umožní vstup.

### Techniky útočníkov:

- **Impersonácia kuriéra**  
"Mám plné ruky, podržíte mi?"
- **Trik so zabudnutou kartou**  
"Zabudol som kartu, pusťte ma, prosím"
- **Stratenie sa v dave**  
Vstup počas rannej špičky
- **Využitie zdvorilosti**  
Počítajú s tým, že odmietnutie je "neslušné"

### Správna reakcia:

- 1 **Asertívne odmietnuť**  
"Prepáčte, ale pravidlá mi zakazujú..."
- 2 **Nasmerovať na recepciu**  
"Prosím, ohláste sa na recepcii"
- 3 **Kontrola zatvorenia dverí**  
Otočiť sa a skontrolovať
- 4 **Spochybnenie neznámych osôb**  
"Môžem vám pomôcť?"
- 5 **Hlásenie - incident nahlásiť na recepcii**

## Dôležité

"Zdvorilé spochybnenie" nie je neslušnosť, ale zodpovednosť

## Zlaté pravidlo

Návštevník sa NIKDY nesmie pohybovať po priestoroch firmy sám a bez dozoru

### Zodpovednosť hostiteľa:

- 1 Registrácia**  
Návšteva sa musí zapísať na recepcii
- 2 Návštevnícky preukaz**  
Viditeľne nosený počas celého pobytu
- 3 Sprevádzanie**  
Od príchodu až po odchod
- 4 Obmedzený prístup**  
Len povolené priestory (zasadačka)
- 5 Ukončenie**  
Odvedenie na recepciu, vrátenie preukazu

### Zakázané oblasti pre návštevy:

- Serverovne a dátové centrá
- Archívy a skladovacie priestory
- Vývojové oddelenia
- Kancelárie s citlivými dátami

### Prečo?

- Prevencia priemyselnej špionáže
- Ochrana citlivých informácií
- Kontrola a audit
- Rýchla evakuácia v núdzi

## Čo je Baiting?

Útočník zanechá na frekventovanom mieste infikované fyzické médium (USB kľúč), ktoré vzbudzuje zvedavosť.

### Scenár útoku:

- 1 Útočník zanechá USB na parkovisku
- 2 Lákavé označenie: "Mzdy Q4 2024", "Dôverné", "Firemná párty"
- 3 Zvedavý zamestnanec ho nájde
- 4 Pripojí do firemného PC
- 5 Automatická inštalácia malvéru
- 6 Kompromitácia siete

### Typy návnad:

- USB kľúče
- Externé disky
- CD/DVD
- Nabíjacie káble

### SPRÁVNY POSTUP:

- 1 **NIKDY** nepripájať
- 2 Odovzdať IT oddeleniu
- 3 IT analyzuje v izolovanom prostredí (sandbox)

### Príklad

Penetračný test: 200 USB na parkovisku. 135 bolo pripojených = 67,5% úspešnosť útoku

## Štatistika

45% ľudí pripojí nájdený USB do počítača

## POŽIAR

### Prevenčia:

- Nepreťažovať zásuvky
- Kontrola káblov
- Voľné únikové cesty
- Prístup k hasiacim prístrojom

### Reakcia:

- Evakuácia
- Aktivácia alarmu
- Volat' 112
- Použiť hasiaci prístroj (ak je to bezpečné)

## VODA

### Scenáre:

- Prasknuté potrubie
- Zatečená strecha
- Havárie klimatizácie
- Zápavy

### Postup:

- BEZPEČNOSŤ - riziko úrazu prúdom
- Odpojenie zariadení (ak je to bezpečné)
- Okamžité hlásenie
- Presun zariadení

## ELEKTRINA

### Pravidlá:

- Len schválené spotrebiče
- Okamžité hlásenie poškodenia
- Zákaz opráv
- Len kvalifikovaný personál

### Výpadok:

- Uloženie práce
- UPS pre kritické systémy
- Čakať na pokyny
- Nereštartovať systémy svojvoľne

## Kľúčové

Pri všetkých environmentálnych hrozbách: BEZPEČNOSŤ ĽUDÍ je priorita č.1

## Čo je bezpečnostný incident?

Akákoľvek udalosť, ktorá ohrozuje alebo by mohla ohroziť bezpečnosť informácií a aktív.

### Príklady incidentov:

- Stratená prístupová karta
- Nájdený cudzí USB kľúč
- Podozrivá osoba v priestoroch
- Kliknutie na phishing odkaz
- Strata/krádež zariadenia
- Neobvyklé správanie PC
- Kolega necháva odomknutý PC
- Únik vody v blízkosti serverov

### Postup hlásenia:

- 1 **KOMU:** IT oddelenie, bezpečnostný manažér, priamy nadriadený, helpdesk
- 2 **KEDY: OKAMŽITE!**
- 3 **ČO: ČO, KDE, KEDY, KTO**
- 4 **AKO:** Bez hanby a obvinení

## Kultúra bezpečného hlásenia

Zamestnanec, ktorý nahlási incident, je **HRDINA**, nie problém!  
Organizácia musí vytvoriť prostredie bez strachu z postihu.

## Kľúčová myšlienka

Bezpečnosť nie je len pravidlá na papieri - vyžaduje **aktívny a viditeľný** prístup vedenia

### Strategická úroveň:

- Bezpečnostné politiky a ich aktualizácia
- Pravidelné hodnotenie rizík
- Investície do infraštruktúry
- Zabezpečenie OOPP

### Praktická úroveň:

- **Ísť príkladom!**
- Pravidelné školenia
- Okamžitá náprava nedostatkov
- Bezpečnostné previerky
- Zahrnutie do hodnotenia výkonu

### Komunikačná úroveň:

- Otvorená komunikácia
- Pravidelné informovanie
- Uznanie a pozitívna motivácia
- Vysvetľovanie "PREČO"

### Ísť príkladom

Ak vedúci používa slabé heslo "heslo123" a nechá PC odomknuté, tím bude robiť to isté

### Dôležité

Bezpečnosť je zodpovednosť **VŠETKÝCH**, ale začína sa od **VRCHU**

- 1 Fyzická a kybernetická bezpečnosť sú neoddeliteľné**  
Slabina v jednej oblasti kompromituje druhú
- 2 Integrovaný bezpečnostný systém je nevyhnutný**  
TZP + Fyzická ochrana + Organizačné opatrenia
- 3 Každý zamestnanec je súčasťou obrany**  
Ste „ľudský firewall“ organizácie
- 4 Jednoduché návyky majú obrovský dopad**  
Zamykanie PC, čistý stôl, hlásenie incidentov
- 5 Súlad nie je voliteľný**  
GDPR, NIS2, ISO 27001 - právne povinnosti
- 6 Kultúra bezpečnosti začína vedením**  
Lead by Example + No-Blame Culture

## Čo môžete urobiť hneď teraz?

### Osobné:

- ✓ Nastaviť auto-lock na 15 min
- ✓ Zapnúť MFA všade, kde je to možné
- ✓ Používať silné, unikátne heslá
- ✓ Zakúpiť privacy filter (ak pracujete verejne)
- ✓ Pravidelne zálohovať dáta
- ✓ Zapnúť šifrovanie disku
- ✓ Cvičiť návyk zamykania PC (Win+L)

### Organizačné:

- ✓ Preskúmať bezpečnostné politiky
- ✓ Zorganizovať školenie pre tím
- ✓ Implementovať Clean Desk Policy
- ✓ Zlepšiť kontrolu návštev
- ✓ Pravidelné bezpečnostné audity
- ✓ Vytvoriť kultúru hlásenia incidentov
- ✓ Vybaviť pracovisko kábl. zámkami

Otázky?