MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 5
SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – BEZPEČNOST Z HLEDISKA LIDSKÝCH ZDROJŮ

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY

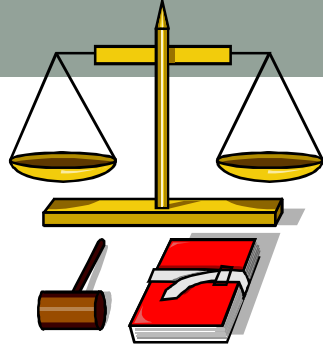
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

- ✓Základní pojmy z oblasti bezpečnosti z hlediska lidských zdrojů
- ✓Před vznikem pracovního vztahu
- ✓ Během pracovního vztahu
- ✓Ukončení nebo změna pracovního vztahu
- ✓Závěr

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Literatura



ČSN ISO/IEC 27000 Datum vydání : 1.5.2010

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Datum vydání : 1.10.2006

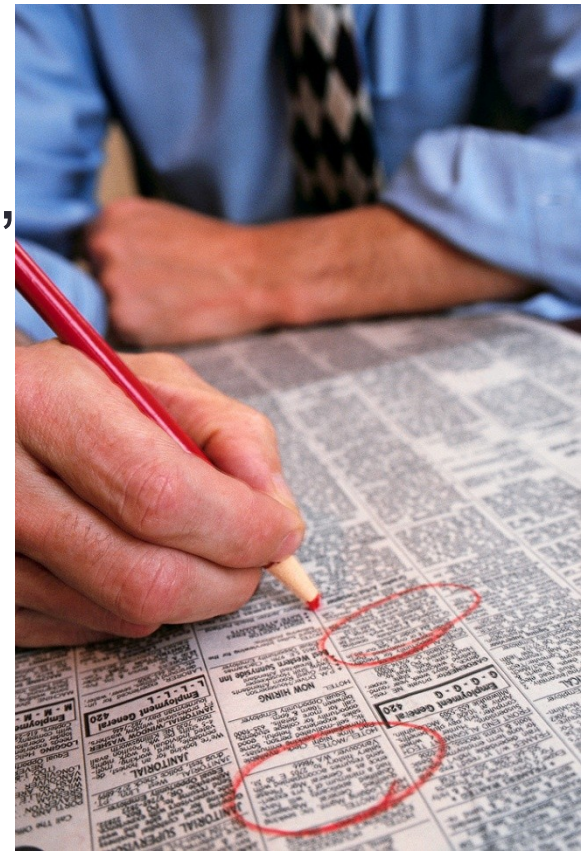
Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

ZÁKLADNÍ POJMY

- vznik pracovního vztahu,
- role a odpovědnosti,
- kandidát uchazeč, zaměstnanec,
- neautorizovaný přístup,
- bezpečnostní událost,
- pracovní smlouva,
- pracovní vztah,
- disciplinární řízení.



1. Před vznikem pracovního vztahu

- **Zajistit**, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti, a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.
- **Odpovědnosti za bezpečnost** by měly být zohledněny v rámci **přijímacího řízení**, měly by být zahrnuty v **pracovních smlouvách a popisech práce**.
- Potenciální uchazeči by měli být náležitě **prověřeni**.

Role a odpovědnosti

Role a odpovědnosti v oblasti bezpečnosti informací by měly zahrnovat:

- požadavek na realizaci a dodržování zásad v souladu s bezpečnostní politikou organizace;
- požadavek na ochranu aktiv před neautorizovaným přístupem, vyzrazením, modifikací, zničením nebo narušením;
- požadavek na vykonávání určitých bezpečnostních procesů nebo činností;
- požadavek na určení jednoznačné odpovědnosti za provedené činnosti;
- požadavek hlásit bezpečnostní události nebo jiná bezpečnostní rizika.

Prověřování

Při prověřování by měl být brán zřetel na dodržení soukromí a ochranu osobních dat a související požadavky předpisů.

Tam, kde je to povoleno, prověrky by měly být prováděny na základě:

- dostupnosti dvou dostatečných referencí, například profesní a osobní;
- kontroly životopisu uchazeče;
- ověření proklamovaného vzdělání a odborné kvalifikace;
- nezávislého ověření totožnosti (cestovním pasem nebo jiným dokladem totožnosti);
- detailnějšího prověření, jako například výpisu z trestního rejstříku, finanční situace, atd.

Podmínky výkonu pracovní činnosti

Pracovní smlouvy by měly být v souladu s bezpečnostní politikou organizace a mimo to také upřesňovat a obsahovat následující:

- všichni zaměstnanci, smluvní a třetí strany by měli podepsat smlouvu o ochraně informací nebo o zachování mlčenlivosti;
- práva a právní odpovědnost zaměstnanců, smluvních stran a ostatních uživatelů;
- odpovědnost za klasifikaci a správu aktiv spojených s informačním systémem a službami zaměstnavatele;
- rozšíření odpovědností i mimo objekt organizace a mimo běžnou pracovní dobu (například v případě vzdálené práce z domova);
- popis kroků, které budou následovat při nedodržení bezpečnostních požadavků ze strany zaměstnanců, smluvních a třetích stran.

2. Během pracovního vztahu

Zajistit, aby si zaměstnanci, smluvní a třetí strany **byli vědomi bezpečnostních hrozeb a problémů** s nimi spojených, svých odpovědností a povinností a aby **byli připraveni podílet se na dodržování** politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

Měly by být **jasně stanoveny odpovědnosti vedoucích zaměstnanců**, aby se zajistilo dodržování bezpečnosti ze strany jednotlivců během celé doby trvání pracovního vztahu

Odpovědnosti vedoucích zaměstnanců

Vedoucí zaměstnanci by měli po uživatelích, smluvních a třetích stranách **požadovat dodržování** bezpečnosti v souladu se zavedenými politikami a postupy.

Nedostatečné seznámení se svými odpovědnostmi za bezpečnost může organizaci způsobit **závažné škody.**

Neschopnost nadřízených dostatečně **motivovat a řídit své podřízené** může vést u zaměstnanců k pocitu, že jejich práce není dostatečně oceněná a důležitá.

Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací

Školení, vzdělávání a zvyšování bezpečnostního povědomí by mělo být uzpůsobeno roli, odpovědnostem a schopnostem dotyčné osoby. Mělo by také zahrnovat informaci o známých hrozbách a postupech při hlášení bezpečnostních incidentů.

Cílem zvyšování bezpečnostního povědomí v rámci školení je naučit jednotlivce **rozpoznávat bezpečnostní incidenty a problémy a reagovat** na ně způsobem, který odpovídá jejich roli.

Disciplinární řízení

Mělo by existovat **formalizované disciplinární řízení** vůči zaměstnancům, kteří se dopustili narušení bezpečnosti.

Disciplinární řízení by **nemělo být zahájeno bez předchozího ověření**, že se opravdu jedná o narušení bezpečnosti.

Disciplinární řízení by mělo působit jako **odstrašující prostředek** odrazující zaměstnance, pracovníky smluvních a třetích stran od porušení bezpečnostních politik, směrnic a od narušení bezpečnosti.

3 Ukončení nebo změna pracovního vztahu

Cílem je zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran **proběhla řádným způsobem**.

Měly by být **určeny jednoznačné odpovědnosti** za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, **za odevzdání přiděleného vybavení a odejmutí přístupových práv**.

Odpovědnosti při ukončení pracovního vztahu

Odpovědnosti a povinnosti platné i po skončení pracovního vztahu by měly být obsaženy ve smlouvách uzavřených se zaměstnanci, smluvními a třetími stranami.

Případné **změny odpovědností** nebo pracovního vztahu by měly být řízeny stejným způsobem jako v případě jejich ukončení.

Za proces a náležitosti spojené s ukončením pracovního vztahu je zpravidla odpovědné **personální oddělení**.

Navrácení zapůjčených prostředků

Při ukončení pracovního vztahu, smluvního vztahu nebo dohody by měli zaměstnanci, pracovníci smluvních a třetích stran **odevzdat veškeré jim svěřené prostředky**, které jsou majetkem organizace.

Mělo by být zajištěno **zálohování a bezpečné smazání informací** uložených na zařízení, které bylo odkoupeno nebo je majetkem zaměstnance, smluvní nebo třetí strany.

Odebrání přístupových práv

- **odejmuta nebo pozměněna přístupová práva** k informacím a prostředkům pro zpracování informací,
- **přezkoumána** přístupová práva k aktivům spojeným s informačními systémy a službami,
- fyzický a logický přístup, klíče, identifikační karty, prostředky pro zpracování informací,
- **změněna veškerá** jim známá **hesla** k aktivním účtům

ZÁVĚR

- Role a odpovědnosti.
- Prověřování.
- Podmínky výkonu pracovní činnosti.
- Bezpečnostní povědomí, vzdělávání a školení.
- Disciplinární řízení.
- Ukončení nebo změna pracovního vztahu.
- Odebrání přístupových práv.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz