



Vyhľásenie o zaručení dostatočnej bezpečnosti informačných systémov s osobnými údajmi zavedením bezpečnostnej politiky

Vedenie Univerzity Mateja Bela v Banskej Bystrici (ďalej len „UMB“) deklaruje na účely bezpečnostnej politiky nasledovné **strategické ciele bezpečnosti**:

1. Vybudovať a trvalo udržiavať vysokú úroveň ochrany a bezpečnosti informačných systémov s osobnými údajmi, najmä v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Výnosom ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov a zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Vytvoriť podmienky a realizovať bezpečné rozmiestnenie najdôležitejších komponentov a trvalo zabezpečovať ich technickú a režimovú ochranu.
3. Obstarávať a implementovať informačné systémy len vysokej kvalitatívnej a odbornej úrovne a úžitkovej hodnoty, ktoré budú vytvárať a ochraňovať dobré meno UMB.
4. Uplatniť pri budovaní bezpečnostného systému princíp vlastníctva.
5. Chrániť osobné údaje a práva zamestnancov, študentov a dodávateľov UMB.
6. Zabezpečiť potrebnú ochranu majetku UMB.
7. Zaviesť systém kontrol výkonu práce a dodržiavania bezpečnostných pravidiel všetkých oddelení, útvarov i samotných zamestnancov s cieľom odhaliť nekvalitný, neprofesionálny alebo inak so záujmami univerzity nezlučiteľný výkon práce.
8. Vytvoriť havarijné plány a plány na obnovu funkčnosti IT zariadení UMB.
9. Vytvoriť a udržiavať funkčnú štruktúru bezpečnosti, ktorá bude zabezpečovať dosiahnutie a udržanie stanovej cielovej úrovne bezpečnosti vo všetkých požadovaných oblastiach.
10. Zaviesť a trvalo zabezpečovať systém hlásení o stave bezpečnostného systému a hlásení o bezpečnostných incidentoch.

Pri návrhoch bezpečnostných opatrení, určených na ochranu kľúčových aktív a ich implementáciu do existujúcich systémov a technologických reťazcov budú uplatňované nasledovné zásady a ciele:

1. **Zásada ochrany dôležitých systémov a komponentov informačného systému**
Dôležité systémy a komponenty informačného systému sú tie časti, ktorých zlyhanie, zničenie alebo iný dôvod nedostupnosti by mal dopad na strategické záujmy UMB. Cieľom je dosiahnuť minimalizáciu rizika zlyhania dôležitých súčastí informačných systémov UMB, komunikačnej a bezpečnostnej infraštruktúry.
2. **Zásada ochrany údajov v informačných systémoch**
Údaje musia byť chránené vo všetkých formách – hlasovej, písomnej a elektronickej, počas ich spracovania a prenosu pomocou počítačov, telefónnej alebo počítačovej siete

a počas ich archivácie. Cieľom je dosiahnuť ekonomicky primeranú a pritom spoľahlivú ochranu osobných a ekonomických údajov, údajov o študentoch a zamestnancoch UMB.

3. Zásada ochrany osôb a personálnej bezpečnosti

Osobami sú zamestnanci UMB, zamestnanci obchodných partnerov UMB, ktorí sa nachádzajú v jej priestoroch a s jej súhlasm. UMB chce a musí chrániť práva osôb, ktorých údaje sú spracúvané. Pre tento účel prijíma opatrenia na ochranu informačných systémov s osobnými údajmi pred neautorizovanou činnosťou neoprávnených osôb alebo pred činnosťou oprávnených zamestnancov majúcich prístup k chráneným údajom, ktorí by chceli tieto oprávnenia zneužiť alebo by mohli takto konať pod nátlakom. UMB má záujem o stabilizáciu kľúčových zamestnancov, najmä tých, ktorí sa podielajú na rozvoji a prevádzke informačných technológií, ktoré podporujúcej jej strategické záujmy.

4. Zásada ochrany hmotného majetku a finančných prostriedkov

Majetok UMB predstavuje značné hodnoty, preto je potrebné zabezpečiť, aby sa s týmito hodnotami nakladalo tak, aby nedošlo k ich poškodeniu, zničeniu alebo iným stratám.

5. Zásada ochrany dobrého mena

Náležitá pozornosť je venovaná ochrane dobrého mena UMB. Cieľom je udržanie a skvalitňovanie svojho dobrého mena.

6. Zásada priradenia zodpovednosti za bezpečnosť

Ochrana aktív UMB je založená na princípe vlastníctva. Vlastníctvom sa v tomto prípade rozumie priradenie informácie, údaju, presne definovanej množiny údajov alebo iného aktíva zamestnancovi, ktorý bude mať osobný záujem na ich ochrane. Každý „vlastník“ aktíva má definované práva a povinnosti, ktoré mu umožnia zabezpečiť spoľahlivú ochranu jemu „zverených“ údajov a aktív.

7. Zásada hlásenia stavu bezpečnostného systému

Vedenie a zamestnanci UMB musia byť pripravení primerane reagovať na krízovú situáciu tak, aby sa minimalizovali jej následky. Činnosť bezpečnostného systému a užívateľov informačného systému je monitorovaná, bezpečnostné incidenty sú sledované a pravidelne vyhodnocované. Proti narušiteľom bezpečostného systému budú zavedené primerané opatrenia v súlade s platnou legislatívou.

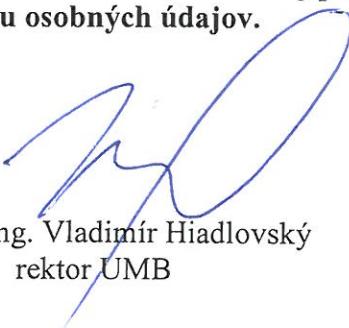
8. Zásada postupu implementácie bezpečnostného systému

Bezpečnostný systém musí byť implementovaný na základe rozpracovaných zásad tak, aby boli rešpektované možnosti a potreby UMB.

Bezpečnostné mechanizmy, ktoré sú alebo budú implementované v prostredí UMB na ochranu aktív, musia mať takú bezpečnostnú úroveň, aby vyhoveli požiadavkám legislatívy Slovenskej republiky a to najmä v oblasti ochrany osobných údajov, ochrany duševného vlastníctva, noriem pre prevádzku a bezpečnosť informačných systémov, ochrany bezpečnosti pri práci, bezpečnosti osôb a majetku.

Toto Vyhlásenie je verejným dokumentom a dokumentom bezpečnostnej politiky UMB v zmysle Bezpečnostného projektu UMB na ochranu osobných údajov.

Banská Bystrica 1. 12. 2017.



doc. Ing. Vladimír Hiadlovský
rektor UMB