SOMI Systems a.s. Banská Bystrica

BEZPEČNOSTNÝ PROJEKT

NÁVRHY OPATRENÍ

Obec Bacúch

Banská Bystrica, marec 2014

Návrhy nových opatrení

Kategória aktív: Počítače, programové vybavenie, operačné systémy

Kategória hrozieb: IT hrozby - vnútorné

Aktívum:	Počítače - PC/Windows
Hrozba:	Použitie neovereného kódu.
Opatrenie:	Zmeniť úroveň prístupových práv používateľov na úroveň USER, pokiaľ to nainštalované softvéry umožňujú. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér.
Aktívum:	Počítače - PC/Windows
Hrozba:	Zničenie konfigurácií.
Opatrenie:	Zvážiť zavedenie zálohovania konfigurácií dôležitých PC na externé dátové úložisko.
Aktívum:	Počítače - PC/Windows
Hrozba:	Zničenie údajov.
Opatrenie:	Vypracovať politiku zálohovania, zabezpečiť pravidelné zálohovanie počítačov, ktoré obsahujú osobné a citlivé údaje. Pre zálohy všetkých počítačov, notebookov a aplikácií zvážiť zriadenie externého dátového úložiska (BackUp server).

Kategória hrozieb: Personálne hrozby - cudzie osoby

Aktívum:	Počítače - PC/Windows
Hrozba:	Krádež.
Opatrenie:	Zaviesť osobnú zodpovednosť zamestnancov za zverené zariadenia.
Aktívum:	Počítače - PC/Windows
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Nastaviť na všetkých počítačoch a aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov. Policy.
Aktívum:	Počítače - PC/Windows
Hrozba:	Únik údajov.
Opatrenie:	Nastaviť na všetkých počítačoch heslo a pravidelne ho meniť. Podpísať zmluvu o mlčanlivosti s externou firmou.

Aktívum:	Prenosné pamäťové médiá
Hrozba:	Krádež.
Opatrenie:	Zabezpečiť šifrovanie prenosných pamäťových médií. Poučiť zamestnancov o rizikách prenosu osobných údajov na pamäťových médiách.

Aktívum:	Prenosné pamäťové médiá
Hrozba:	Únik údajov.
Opatrenie:	Zabezpečiť šifrovanie prenosných pamäťových médií. Poučiť zamestnancov o rizikách prenosu osobných údajov na pamäťových médiách.

Aktívum:	Služby pripojenia k internetu
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača. Pravidelne meniť heslá.

Kategória hrozieb: Personálne hrozby - vlastný personál

Aktívum:	Počítače - PC/Windows
Hrozba:	Chyby a nekvalita údržby
Opatrenie:	Podpísať zmluvy o mlčanlivosti s externým technikom.

Aktívum:	Počítače - PC/Windows
Hrozba:	Neautorizované postupy a činnosti.
Opatrenie:	Zmeniť úroveň prístupových práv používateľov na úroveň USER, pokiaľ to nainštalované softvéry umožňujú. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér. Zaviesť kontrolu sťahovaných súborov z Internetu podľa príloh.

Aktívum:	Počítače - PC/Windows
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Nastaviť na všetkých počítačoch a aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov. Zvážiť zavedenie autorizácie prístupu do siete napr. prostredníctvom Active Directory a Domain Policy.

Aktívum:	Počítače - PC/Windows
Hrozba:	Neúmyselné poškodenie
Opatrenie:	Zmeniť úroveň prístupových práv používateľov na úroveň USER, pokiaľ to nainštalované softvéry umožňujú. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér.

Aktívum:	Počítače - PC/Windows
Hrozba:	Úmyselné poškodenie
Opatrenie:	Zamestnancom nastaviť prístupové práva na úroveň USER, pokiaľ to nainštalovaný softvér umožňuje. Nastaviť na všetkých počítačoch heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum:	Prenosné pamäťové médiá
Hrozba:	Nelegálne zhromažďovanie údajov.
Opatrenie:	Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov.

Aktívum:	Prenosné pamäťové médiá
Hrozba:	Únik údajov.
Opatrenie:	Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov.

Aktívum:	Služby pripojenia k internetu
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača. Pravidelne meniť heslo, poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum:	Služby pripojenia k internetu
Hrozba:	Neúmyselné poškodenie
Opatrenie:	Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača. Pravidelne meniť heslá.

Aktívum:	Služby pripojenia k internetu
Hrozba:	Úmyselné poškodenie
Opatrenie:	Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača.

Aktívum:	Tlačiarne a iné výstupné periférie
Hrozba:	Nelegálne zhromažďovanie údajov.
Opatrenie:	Obmedziť možnosť zmeniť si tlačiareň mimo kanceláriu a tým zabrániť nechcenému vytlačeniu citlivých dát mimo dosahu. Zamedziť zamestnancom zdieľanie tlačiarne, ktoré majú pripojené k počítaču.

Aktívum: Tlačiarne a iné výstupné periférie

Hrozba: Únik údajov.

Opatrenie: Obmedziť možnosť zmeniť si tlačiareň mimo kanceláriu. Zamedziť zamestnancom zdieľanie tlačiarne, ktoré majú pripojené k počítaču.

Kategória hrozieb: Technické, technologické hrozby

Aktívum: Počítače - PC/Windows

Hrozba: Výpadky elektrickej energie

Opatrenie: Zabezpečiť záložné zdroje pre všetky dôležité počítače.

Kategória aktív: Komunikačná infraštruktúra

Kategória hrozieb: Ostatné, nešpecifikované hrozby

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Nevhodné umiestnenie

Opatrenie: Umiestniť zariadenia do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - rozvody

Hrozba: Nevhodné umiestnenie

Opatrenie: Umiestniť voľne prístupnú dátovú kabeláž do ochranných líšt. Vypracovať plán kabeláže, prepojenia aktívnych prvkov a zásuviek.

Kategória hrozieb: Personálne hrozby - cudzie osoby

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Neidentifikovaný vstup.

Opatrenie: Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Únik údajov.

Opatrenie: Zvážiť umiestnenie zariadení do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - rozvody

Hrozba: Neúmyselné poškodenie.

Opatrenie: Vypracovať plán kabeláže a prepojenia aktívnych prvkov a zásuviek. Umiestniť voľne prístupnú dátovú kabeláž do ochranných líšt.

Aktívum: Počítačová sieť - rozvody

Hrozba: Úmyselné poškodenie.

Opatrenie: Vypracovať plán kabeláže a prepojenia aktívnych prvkov a zásuviek. Umiestniť voľne prístupnú dátovú kabeláž do ochranných líšt.

Kategória hrozieb: Personálne hrozby - vlastný personál

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Krádež

Opatrenie: Umiestniť zariadenia do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Neidentifikovaný vstup.

Opatrenie: Umiestniť zariadenia do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - aktívne prvky

Hrozba: Únik údajov.

Opatrenie: Umiestniť zariadenia do uzamykateľného dátového rozvádzača.

Aktívum: Počítačová sieť - rozvody

Hrozba: Neúmyselné poškodenie

Opatrenie: Vypracovať plán kabeláže a prepojenia aktívnych prvkov a zásuviek. Umiestniť voľne prístupnú dátovú kabeláž do ochranných líšt.

Aktívum: Počítačová sieť - rozvody

Hrozba: Úmyselné poškodenie

Opatrenie: Vypracovať plán kabeláže a prepojenia aktívnych prvkov a zásuviek. Umiestniť voľne prístupnú dátovú kabeláž do ochranných líšt.

Kategória aktív: Údaje, informácie

Kategória hrozieb: IT hrozby - vnútorné

Aktívum: Elektronický informačný systém - MADE

Hrozba: Odmietnutie služby.

Opatrenie: Vyradiť z prevádzky morálne zastarané a potenciálne nebezpečné zariadenia.

Aktívum:	Elektronický informačný systém - MADE
Hrozba:	Zničenie údajov.
Opatrenie:	Vypracovať politiku zálohovania, pre zálohovanie údajov z IS a aplikácií, zvážiť zriadenie samostatného servera, externého dátového úložiska (BackUp Server), ktoré sa bude nachádzať v inej miestnosti, fyzicky oddelené od servera.

Aktívum:	Osobné údaje - kancelárske aplikácie
Hrozba:	Zničenie údajov.
Opatrenie:	Vypracovať politiku zálohovania, pre zálohovanie údajov z IS a aplikácií, zvážiť zriadenie samostatného servera, externého dátového úložiska (BackUp Server), ktoré sa bude nachádzať v inej miestnosti, fyzicky oddelené od servera.

Kategória hrozieb: Personálne hrozby - cudzie osoby

Aktívum:	Elektronický informačný systém - MADE
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Nastaviť vo všetkých aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov. Podpísať zmluvu o mlčanlivosti s externým informatikom.

Aktívum:	Elektronický informačný systém - MADE
Hrozba:	Únik údajov.
Opatrenie:	Nastaviť vo všetkých aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum:	Osobné údaje - kancelárske aplikácie
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Nastaviť vo všetkých aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov. Podpísať zmluvu o mlčanlivosti s externým informatikom.

Aktívum:	Osobné údaje - papierová forma
Hrozba:	Krádež.
Opatrenie:	Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje.

Aktívum:	Osobné údaje - papierová forma
Hrozba:	Neúmyselné poškodenie.
Opatrenie:	Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi.

Aktívum: Osobné údaje - papierová forma

Hrozba: Úmyselné poškodenie.

Opatrenie: Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi.

Aktívum: Osobné údaje - papierová forma

Hrozba: Únik údajov.

Opatrenie: Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje.

Kategória hrozieb: Personálne hrozby - vlastný personál

Aktívum: Elektronický informačný systém - MADE

Hrozba: Neautorizované postupy a činnosti.

Opatrenie: Nastaviť všetkým zamestnancom prístupové práva na úrovni USER. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér. Zaviesť kontrolu sťahovaných súborov z Internetu podľa príloh.

Aktívum: Elektronický informačný systém - MADE

Hrozba: Neidentifikovaný vstup.

Opatrenie: Nastaviť v aplikácií heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum: Elektronický informačný systém - MADE

Hrozba: Nelegálne zhromažďovanie údajov.

Opatrenie: Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov.

Aktívum: Elektronický informačný systém - MADE

Hrozba: Únik údajov.

Opatrenie: Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov. Obmedziť možnosť zmeniť si tlačiareň mimo kancelárie.

Aktívum: Osobné údaje - kancelárske aplikácie

Hrozba: Neautorizované postupy a činnosti.

Opatrenie: Zmeniť úroveň prístupových práv používateľov na úroveň USER, pokiaľ to nainštalované softvéry umožňujú. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér. Zaviesť kontrolu sťahovaných súborov z Internetu podľa príloh.

Aktívum:	Osobné údaje - kancelárske aplikácie
Hrozba:	Neidentifikovaný vstup.
Opatrenie:	Nastaviť v aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum:	Osobné údaje - kancelárske aplikácie
Hrozba:	Nelegálne zhromažďovanie údajov.
Opatrenie:	Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov.

Aktívum:	Osobné údaje - kancelárske aplikácie
Hrozba:	Únik údajov.
Opatrenie:	Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo nastaviť politiku používania týchto zariadení napr. pomocou softvéru (NOD32,OptimAccess,...) alebo na úrovni registrov. Obmedziť možnosť zmeniť si tlačiareň mimo kanceláriu.

Aktívum:	Osobné údaje - papierová forma
Hrozba:	Nelegálne zhromažďovanie údajov.
Opatrenie:	Zamedziť zdieľaniu tlačiarní mimo kancelárie a tým zabrániť nechcenému vytlačeniu citlivých dát mimo dosahu. Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi

Aktívum:	Osobné údaje - papierová forma
Hrozba:	Neúmyselné poškodenie
Opatrenie:	Zabezpečiť uzamykateľné skrine pre citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi

Aktívum:	Osobné údaje - papierová forma
Hrozba:	Úmyselné poškodenie
Opatrenie:	Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi

Aktívum: Osobné údaje - papierová forma

Hrozba: Únik údajov.

Opatrenie: Zamedziť zdieľaniu tlačiarní mimo kancelárie a tým zabrániť nechcenému vytlačeniu citlivých dát mimo dosahu. Zabezpečiť uzamykateľné skrine pre všetky citlivé a osobné údaje. Dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi.

Kategória aktív: Personál, zamestnanci a osoby

Kategória hrozieb: Personálne hrozby - cudzie osoby

Aktívum: Zamestnanci administratívy a výkonní pracovníci

Hrozba: Únik údajov.

Opatrenie: Zvážiť zavedenie autorizácie prístupu do siete napr. prostredníctvom Active Directory a Domain Policy.

Kategória hrozieb: Personálne hrozby - vlastný personál

Aktívum: Zamestnanci administratívy a výkonní pracovníci

Hrozba: Nespokojnosť.

Opatrenie: Monitorovať druh a príčinu nespokojnosti, prijať opatrenia na úrovni zmeny štruktúry pracovných tímov, prípadne adresnejšieho ohodnotenia zamestnancov.

Aktívum: Zamestnanci administratívy a výkonní pracovníci

Hrozba: Neúmyselné poškodenie

Opatrenie: Zmeniť úroveň prístupových práv používateľov na úroveň USER, pokiaľ to nainštalované softvéry umožňujú. Zamedziť zamestnancom možnosť inštalovať si vlastný softvér. Zaviesť kontrolu sťahovaných súborov z Internetu podľa príloh.

Aktívum: Zamestnanci administratívy a výkonní pracovníci

Hrozba: Úmyselné poškodenie

Opatrenie: Nastaviť na všetkých počítačoch a aplikáciách heslo a pravidelne ich meniť. Používať pravidlá hesiel (Password Policy), poučiť zamestnancov o dodržiavaní pravidiel hesiel a o rizikách prezradenia svojich prihlasovacích údajov.

Aktívum: Zamestnanci administratívy a výkonní pracovníci

Hrozba: Únik údajov.

Opatrenie: Zamedziť zamestnancom možnosť používania vlastných USB zariadení alebo zabezpečiť kontrolované používanie týchto zariadení napr. pomocou softvéru OptimAccess alebo na úrovni registrov.

Kategória aktív: Prostredie, budovy a ich zariadenia

Kategória hrozieb: Personálne hrozby - cudzie osoby

Aktívum: Archív dokumentov - registratúrne stredisko

Hrozba: Neidentifikovaný vstup.

Opatrenie: Odporúča sa zaviesť kľúčový režim. Archív zabezpečiť bezpečnostným kovaním.

Kategória hrozieb: Personálne hrozby - vlastný personál

Aktívum: Archív dokumentov - registratúrne stredisko

Hrozba: Neidentifikovaný vstup.

Opatrenie: Odporúča sa zaviesť kľúčový režim. Archív zabezpečiť bezpečnostným kovaním.

Aktívum: Archív dokumentov - registratúrne stredisko

Hrozba: Únik údajov.

Opatrenie: Odporúča sa zaviesť kľúčový režim. Archív zabezpečiť bezpečnostným kovaním.

Kategória hrozieb: Technické, technologické hrozby

Aktívum: Administratívne priestory organizácie

Hrozba: Výpadky elektrickej energie

Opatrenie: Zabezpečiť záložné zdroje pre všetky dôležité zariadenia.

Aktívum: Archív dokumentov - registratúrne stredisko

Hrozba: Požiar

Opatrenie: Zabezpečiť priestory archívu protipožiarnym zariadením.