Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Popis havárie	**Návrh preventívnych opatrení**	**Postupy na zabezpečenie stavu obnovy**
1.Porucha PC spôsobená vírusom, neautorizovaným programom	● Zabezpečiť antivírovú ochranu ● Inštalovať len autorizované programy oprávnenými zamestnancami ● Preverovať cudzie nosiče (USB, CD ROM ...) ● Nepripájať nepreverené PC bez vedomia admin do LAN ● Nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN ● Neotvárať nevyžiadané e-mailové prílohy ● Nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou ● Nesťahovať neautorizované programy z prostredia internetu ● Sledovať aktuálne dianie na LAN a v sieti internet	● Odpojiť každého užívateľa ● Spustiť antivírový program s aktuálnou DB vírusov ● detekovať spôsob narušenia ● odstrániť príčiny ● opraviť narušenú funkčnosť ● opätovne skontrolovať systém antivírovým programom ● prekontrolovať všetky PC ● nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie
2. Porucha napájania, strata dodávky elektrickej energie	● Dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia	● V čase výpadku sa musí záložný zdroj automaticky aktivovať
3. Porucha prostriedkov demilitarizovanej zóny	● Monitorovať činnosť zariadení ● Monitorovať funkčnosť všetkých zariadení ● Zabezpečiť prístup len pre pracovníkov s oprávnením ● Periodicky meniť administrátorské a užívateľské prístupy s heslami ● Zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu ● Zabezpečiť programovú aktuálnosť ● Zabezpečiť technickú aktuálnosť ● Kontrolovať súbory zaznamenávajúce činnosť systému ● Kontrolovať súbory	V prípade narušenia ● Odpojiť LAN od prostriedkov demilitarizovanej zóny ● Vyhľadať príčinu nefunkčnosti ● Odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku ● Poveriť prostriedky firewallu, prekladu adries (DNS) a proxy ● Po otestovaní funkčnosti pripojiť LAN
4. Porucha aktívnych prvkov siete	● Monitorovať činnosť ● Zabezpečiť dostatočnú kapacitu ● Pripájať ich prostredníctvom záložného zdroja ● Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom	● Vymeniť nefunkčnú časť
5. Porucha pasívnej	● Premeranie kabeláže, zásuviek	● Opraviť prípadne vymeniť

časti siete	a konektorov	vadnú časť
6. Havária databáz	● Sledovať konfiguračné súbory ● Monitorovať hlásenia programov a včas na ne reagovať ● Denne kontrolovať chybové hlásenia aplikácie a databázy	● Po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy
7. Havária aplikácie	● Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov ● Sledovať konfiguračné súbory ● Monitorovať hlásenia a včas na ne reagovať ● Denne kontrolovať chybové hlásenia aplikácie a databázy	● Preinštalovať aplikáciu ● Nainštalovať novšiu verziu aplikácie ● Konzultovať chyby s dodávateľom
8. Porucha mail servera	● Sledovať konfiguračné súbory ● Monitorovať hlásenia a včas na ne reagovať ● Denne kontrolovať chybové hlásenia ● Nainštalovať antivírovú ochranu ● Zálohovať systém – obraz disku	● Vymeniť nefunkčnú časť ● Aktualizovať softvér ● V prípade výmeny disku previesť inštaláciu zo zálohy
9. Porucha pracovných staníc	● Používať len autorizované programy ● Inštalovať antivírové programy ● Inštalovať nové programy smie len poverený zamestnanec ● Užívatelia nesmú zasahovať do konfiguračných súborov ● Chybové hlásenia sú povinný hlásiť správcovi systému ● Zálohovať dáta na určené média ● Za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec	● Technická chyba – zabezpečiť opravu nefunkčnej časti ● Softvérova chyby – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu
10. Narušenie dverí, okien	● Pravidelne sledovať funkčnosť	● Neodkladne zabezpečiť opravu ● Hľadať príčinu a odstrániť
11. Narušenie monitorovaného objektu	● Pravidelne sledovať funkčnosť	● Hľadať a eliminovať príčinu narušenia
12.Mimoriadne udalosti spôsobené vplyvom zvyškových rizík	● Vybudovať komplexný záložný systém mimo priestorov budovy v bezpečnej vzdialenosti ● Zabezpečiť niekoľkonásobné záložne kópie ● Vytvorenie chráneného komunikačného dátového kanálu na záložne pracovisko ● Zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti ● Kontrolovať, či sú splnené protipožiarne opatrenia ● Kontrolovať osoby pri vstupe do budovy ● Vo vytipovaných priestoroch inštalovať EZS, bezpečnostné	V prípade vyradenia IS z činnosti ● Zvolať krízový štáb ● Koordinovať činnosť podľa havarijných smerníc ● Aktivovať záložne pracovisko ● Skontrolovať úplnosť systému na záložnom pracovisku ● Spustenie záložnej prevádzky ● Odstránenie škôd na pôvodnom pracovisku ● Po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko V prípade napadnutia len časti IS ● Presunúť aktíva do vyhovujúcich priestorov

	mreže, dvere ● Zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov	● Inštalovať záložne databázy a pripojenia ak sú nutné ● Spustiť prevádzku ● Po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou