„Optimalizácia systému riadenia informačnej bezpečnosti“ – závery aktivity 2.2

Cieľom aktivity bolo implementovať systém manažérstva informačnej bezpečnosti podľa požiadaviek normy ISO/IEC 27001 na podporu vnútorného systému zabezpečovania kvality na Pedagogickej fakulte Katolíckej univerzity v Ružomberku;

- Identifikácia výstupu:
  - Príručka systému manažérstva informačnej bezpečnosti;
  - Prehlásenie o aplikovateľnosti;
  - Politika informačnej bezpečnosti organizácie;
  - Výsledky analýzy rizík a návrhy na eliminovanie hrozieb a rizík;
  - Smernice a procedúry systému informačnej bezpečnosti;
  - Závery z preskúmania systému vedením organizácie;
  - Záznamy incidentov a hrozieb a závery z ich vyhodnotenia;
  - Záznamy o meraní parametrov výkonnosti systému.
- Identifikácia činností
  - 2.2.1 Preskúmanie súčasnej úrovne plnenia požiadaviek normy ISO/IEC 27001;
  - 2.2.2 Prekonanie nezhôd medzi požiadavkami normy a súčasným stavom prostredníctvom navrhnutých opatrení;
  - 2.2.3 Implementácia systému a vyškolenie určených zamestnancov;
  - 2.2.4 Preskúmanie funkčnosti systému manažérstva informačnej bezpečnosti internými auditmi;
  - 2.2.5 Vyhodnotenie preskúmania systému a realizácia opatrení vyplývajúcich z vyhodnotenia;
  - 2.2.6 Zhrnutie poznatkov z budovania systému informačnej bezpečnosti pre univerzitné pracoviská.
- Identifikácia rizík – keďže aktivita bola pomerne závislá na využití hardvérových prostriedkov, ako potenciálne riziká boli identifikované:
  - Oneskorenie v procese verejného obstarávania;
  - Obchodné riziká - procesy súvisiace s objednávaním a dodávaním navrhovaného riešenia;
  - Technické riziká - pri overovaní funkcionality riešenia zmodernizovaných zariadení počas skúšobnej prevádzky;
  - Projektové riziká - týkajúce sa riadenia projektu, dodržania časových harmonogramov, rozpočtovaných nákladov vychádzajúcich z aktuálnych ponúk.

  Opatrenia na minimalizáciu rizík:

  - systematická identifikácia, evidencia a monitorovanie možných rizík;
  - dôkladná príprava verejného obstarávania v súlade s metodickými usmerneniami ÚVO;
  - zmluvne zabezpečenie záväzných podmienok pre dodávateľov, zabezpečiť funkčnosť dodávaných zariadení dôkladným a opakovaným preskúšaním funkčnosti;

- dôkladne premyslený harmonogram jednotlivých krokov na základe konzultácie dodávateľa so zodpovedným riešiteľom vrátene dôkladného preverenia schopnosti a zručnosti pracovníkov;
- uplatňovanie zásad manažmentu kvality a opatrení na znižovanie rizík počas trvania celého projektu;
- uplatňovanie zásad projektového manažmentu a opatrení na znižovanie rizík počas trvania projektu.

- Identifikácia kritických faktorov úspechu – zahrnutie všetkých aktív a úzka spolupráca s vlastníkmi aktív/rizík, podobne sa ako kritický faktor ukázala spolupráca s riešiteľmi aktivity 2.3, úlohy bolo výhodné správne synchronizovať.

Základné pripomienky:

- Pozitívne – preukázateľne vysoká miera zapojenia manažmentu a akademickej obce do tejto najrozsiahlejšej aktivity;
- Vyčlenenie potrebných ľudských zdrojov pre riešenie informačnej bezpečnosti sa javí ako kľúčové pre udržateľnosť dosiahnutých výsledkov v oblasti manažérstva informačnej bezpečnosti;
- Norma ISO/IEC 27001 bola v priebehu riešenia revidovaná (rok 2013), aktivita sa začala realizovať podľa postupu vtedy platnej normy, do ukončenia aktivity sa časť výstupov prispôsobila revidovanej norme;
- Ide o jediný systém manažérstva v rámci všetkých implementovaných systémov podporujúcich vnútorný systém zabezpečovania kvality, ktorý stanovuje požiadavky, a teda je certifikovateľný. Chýba stanovisko vedenia PF KU týkajúce sa zámerov v tejto oblasti a taktiež lepšia previazanosť na iné systémy manažérstva PF KU.

Očakávania:

- Spoznanie rizík v oblasti informačnej bezpečnosti na PF KU;
- Navrhnutie pravidiel a postupov pre dosiahnutie požadovanej úrovne IB;
- Implementovanie navrhnutého systému SMIB do prostredia PF KU;
- Zvýšenie povedomia zamestnancov PF KU o dôležitosti SMIB.