Politika řízení kontinuity činností

I. Úvodní ustanovení

1) Politika řízení kontinuity činností stanovuje pravidla pro minimalizaci ztrát způsobených možnými haváriemi (požár, výbuch plynu, přerušení dodávek elektrické energie, výpadek výpočetních kapacit či komunikačních kanálů, nedostupnost externích služeb, teroristický útok atd.) nebo přírodními vlivy (například povodeň, přívalový déšť, úder blesku, vichřice) a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„zákon o kybernetické bezpečnosti"*) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„vyhláška o kybernetické bezpečnosti"*) v podmínkách Univerzity Hradec Králové (dále také *„UHK"*).
2) Účelem této politiky je:
   a) stanovit práva a povinnosti zúčastněných osob,
   b) stanovit cíle řízení kontinuity činností s ohledem na minimální úroveň poskytovaných služeb, dobu obnovení chodu IS a bodu obnovení dat,
   c) stanovit způsoby hodnocení dopadů kybernetických bezpečnostních událostí na kontinuitu a posuzování souvisejících rizik,
   d) určit obsah plánů kontinuity činností a havarijních plánů jednotlivých IS,
   e) nastavit a zavést postupy pro realizaci opatření vydaných Národním úřadem pro kybernetickou a informační bezpečnost (dále také *„NÚKIB"*).
3) Tato politika je závazná pro zaměstnance UHK, kteří se podílejí na správě a provozu informačních systémů UHK v rámci své působnosti.

II. Práva a povinnosti zúčastněných osob

1) Zúčastněnými osobami se rozumí bezpečnostní role dle *Politiky organizační bezpečnosti* a uživatelé IS.
2) Práva a povinnosti zúčastněných osob v oblasti kybernetické bezpečnosti vyplývají ze systému řízení bezpečnosti informací (dále také jen *„SŘBI"*) a dalších vnitřních předpisů UHK.
3) Výkon práv a povinností zúčastněných osob je podmíněn strukturou zdrojů, nastavením postupů a činností v rámci správy a provozu prvků informačních a komunikačních technologií UHK.

III. Cíle řízení kontinuity činností

1) Cílem řízení kontinuity činností je:

   a) stanovit na základě výstupů hodnocení rizik a analýzy dopadů minimální rozsah poskytovaných služeb jednotlivých agend významných informačních systému (dále také „*VIS*") UHK,

   b) zajistit bezpečnost a kontinuitu poskytování služeb informačních a komunikačních technologií i v podmínkách vzniku kybernetického bezpečnostního incidentu, kybernetické bezpečnostní události, mimořádné události nebo v případě narušení poskytování služeb informačních a komunikačních technologií,

   c) zahájit kroky směřující k zajištění obnovy služeb na požadovanou úroveň,

   d) minimalizovat škody na majetku nebo aktivech VIS UHK, vzniklé v důsledku mimořádné události.

2) Procesy kontinuity činností jsou řízeny a dokumentovány.

3) Každé primární aktivum má stanovenu dobu obnovení chodu (RTO) a bod obnovení dat (RPO).

Minimální úroveň poskytovaných služeb

4) Minimální úrovní poskytovaných služeb se rozumí minimální rozsah služeb prvků informačních a komunikačních technologií pro užívání, provoz a správu IS.

Doba obnovení chodu

5) Dobou obnovení chodu se rozumí doba, kdy prvky informačních a komunikačních technologií dosáhnou stanovené úrovně poskytovaných služeb.

Bod obnovení dat

6) Bodem obnovení dat se rozumí okamžik, ke kterému jsou zpětně obnovena data na příslušnou úroveň poskytovaných služeb.

7) Bodem plného obnovení dat se rozumí okamžik, ke kterému jsou plně obnovena data.

IV. Politika řízení kontinuity činností pro naplnění cílů kontinuity

1) Pro naplnění cílů kontinuity jsou aplikačními správci vypracovány, řízeny a pravidelně aktualizovány plány kontinuity činností a havarijní plány prvků informačních a komunikačních technologií a souvisejících služeb.

2) Plány kontinuity činností a havarijní plány jsou pravidelně testovány.

V. Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik

Hodnocení dopadů kybernetického bezpečnostního incidentu na kontinuitu a posuzování souvisejících rizik je součástí analýzy dopadů v rámci hodnocení primárních aktiv a jejich

vazeb na podpůrná aktiva. Při stanovení hodnoty aktiv a navazujících rizik je nutno brát v úvahu i dopad na zajištění kontinuity činností daného aktiva.

VI. Určení a obsah potřebných plánů kontinuity a havarijních plánů

1) Plán kontinuity činností a havarijní plán jsou pro IS zahrnuty ve společném dokumentu.
2) Tento dokument obsahuje zejména:
   a) hodnotu aktiv a stanovení dopadů a rizik souvisejících s ohrožením kontinuity činností,
   b) minimální úroveň poskytovaných služeb,
   c) dobu obnovení chodu na minimální úroveň poskytovaných služeb,
   d) bod obnovení dat na dosažení minimální úrovně poskytovaných služeb,
   e) dobu obnovení chodu na plnou úroveň poskytovaných služeb,
   f) bod obnovení dat na dosažení plné úrovně poskytovaných služeb,
   g) popis vazeb mezi jednotlivými prvky informačních a komunikačních technologií,
   h) finanční, technické, lidské a informační zdroje nutné pro realizaci,
   i) pravidla pro aktualizaci a plány testování,
   j) opatření použitá k zabránění vzniku kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu,
   k) postupy v případě výskytu kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu a mimořádné události,
   l) odpovědnosti jednotlivých zúčastněných osob,
   m) časové posloupnosti činností,
   n) návaznosti na havarijní plány jiných IS.

VII. Postupy pro realizaci opatření vydaných NÚKIB

Na realizaci opatření vydaných NÚKIB se použijí pravidla dle této politiky.

VIII. Závěrečná ustanovení

Politika řízení kontinuity činností vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor