Univerzita Hradec Králové

Politika zálohování a obnovy a dlouhodobého ukládání

I. Úvodní ustanovení

1) Politika zálohování a obnovy a dlouhodobého ukládání stanovuje principy a procesy zálohování dat i zálohování prostředků pro zpracování informací 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 stanovit postupy pro provádění, udržování a testování záloh, pro případ obnovy dat ze záloh jako následek kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události.

3) Tato politika je závazná pro všechny aplikační správce významných informačních systémů (dále také *„VIS*") a provozně kritických aktiv, které je nutné zahrnout při plánování, vytváření a testování záloh a v procesu obnovování ze záloh.

II. Požadavky na zálohování a obnovu

1) Garant podpůrného aktiva stanoví požadavky na zálohování pro každé informační aktivum VIS. Minimální požadavky na zálohování a obnovu jsou:

   a) rozsah zálohování,

   b) Doba obnovy chodu (Recovery Time Objective – RTO) se rozumí doba, kdy prvky informační a komunikační technologie dosáhnou stanovené úrovně poskytovaných služeb,

   c) Bod obnovy dat (Recovery Point Objective – RPO) se rozumí okamžik, ke kterému jsou zpětně obnovena data.

2) Požadavky na zálohování realizuje aplikační správce VIS minimálně v těchto oblastech:
   a) příprava *Plánu zálohování*,
   b) řízení kapacit pro zálohování,
   c) provádění záloh a obnovy a aktualizace *Plánu zálohování*,
   d) kontrola záloh,
   e) test obnovy.

III. Pravidla a postupy zálohování

1) Každý klíčový prvek informační a komunikační technologie má zpracován *Plán zálohování*, který obsahuje minimálně:
   a) základní popis a rozsah zálohování,
   b) stanovení RTO a RPO,
   c) předpokládaný objem zálohovaných dat,
   d) určení způsobu zálohy,
   e) dobu uchování (retence) záloh,
   f) umístění záloh,
   g) zabezpečení zálohovacích řešení,
   h) stanovení způsobu testů obnovy ze záloh.
2) Proces zálohování je monitorován. Aplikační správce VIS zodpovídá za úspěšnost procesu zálohování.
3) Data musí být uchovávána v souladu s platnou legislativou určující například dobu jejich uchování, případně, pokud se jedná o osobní údaje, způsoby nakládání s nimi (skartace).

IV. Pravidla a postupy dlouhodobého ukládání

1) Zálohy pro dlouhodobé ukládání nejsou ukládány na zařízení zálohovaného IS.
2) Zálohy pro dlouhodobé ukládání jsou ukládány mimo lokalitu primárního úložiště dat.
3) Úložiště dlouhodobých záloh splňují pravidla fyzické bezpečnosti.
4) Vstup osob do prostor se zálohami je řízen a omezen pouze na oprávněné osoby.

V. Pravidla bezpečného zálohování a dlouhodobého ukládání informací

1) Dlouhodobé ukládání je řešeno dle požadavků Garantů podpůrných aktiv minimálně v rozsahu:
   a) doba ukládání informací včetně archivace,
   b) způsob přístupu k archivovaným datům,
   c) způsob likvidace dat.

2) Dlouhodobé ukládání informací a zálohovacích médií zabezpečuje aplikační správce VIS na základě požadavků Garanta podpůrného aktiva.

3) Pravidla bezpečného zálohování a dlouhodobého ukládání informací jsou stanovena v *Plánu zálohování*.

VI. Pravidla a postupy obnovy

1) Postupy obnovy obsahují popis procesu obnovy a jsou součástí *Plánu zálohování*.

2) Pravidla obnovy obsahují minimálně:

   a) rozsah obnovy,

   b) zdroj obnovy,

   c) cíl obnovy,

   d) test obnovy.

VII. Pravidla a postupy testování zálohování a obnovy

1) Plány kontrol čitelnosti, úplnosti a obnovy dat ze záloh jsou součástí *Plánu zálohování*.

2) Provedení testů obnovy dat ze zálohy je dokumentováno.

3) Provedením testů obnovy dat nelze narušit provoz žádného prvku informační a komunikační technologie.

4) V případě zjištění chyb při testu je nutno přijmout opatření k nápravě.

VIII. Politika přístupu k zálohám, ukládaným informacím

K zálohovacím médiím mají přístup pouze osoby provádějící zálohování. Ostatní osoby mohou v případě odůvodněné potřeby získat přístup k zálohám na základě povolení Manažera kybernetické bezpečnosti (dále také *„Manažer KB*").

IX. Závěrečná ustanovení

Politika zálohování a obnovy a dlouhodobého ukládání vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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