Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-009**
Název dokumentu:	**Politika zálohování a obnovy a dlouhodobého ukládání**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politiku je nutno aplikovat na všechny správce VISů a provozně kritických aktiv, které je nutné zahrnout při plánování, vytváření a testování záloh a v procesu obnovování ze záloh. Rovněž se aplikuje na osoby zodpovědné za SLA služeb (a jejich dat), které budou zálohované.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 6, 10, 15, 19
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	4 + 0
Verze:	1.1
Význam a benefity:	Tato politika stanovuje postupy pro provádění, udržování a testování záloh, pro případ obnovy dat ze záloh jako následek bezpečnostního incidentu.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

Záložní soubor je kopie souborů a programů vytvořených pro usnadnění obnovy.

Dopady ztráty dat mohou zahrnovat jeden nebo více z následujících:

- ztráta produktivity;
- právní dopady;
- ztráta dobrého jména.

Provozní servery a jejich data, která organizace vlastní nebo spravuje, jsou klasifikovány. Klasifikace následně určí parametry zálohování.

a) Požadavky na zálohování a obnovu

Návrh informačního nebo komunikačního systému musí obsahovat požadavky na zálohování (tzv. Plán záloh), které musí být ve shodě s SLA parametry (tedy dostupností) informačního nebo komunikačního systému. Musí být určeno, kdo a jakým způsobem Plán záloh schvaluje. Vždy se požaduje vytvoření detailního návrhu zálohování celého informačního nebo komunikačního systému.

Distribuce záloh a typ zálohovacích médií odpovídá pravidlu 3-2-1. Toto pravidlo znamená, že jsou k dispozici tři kopie dat na dvou různých typech médií, přičemž alespoň jedno z nich se nachází mimo lokalitu umístění informačního nebo komunikačního systému („offsite“). Za dodržení pravidla zodpovídá správce zálohování.

b) Pravidla a postupy zálohování

Při vytváření pravidel a postupů zálohování je třeba vzít v úvahu následující aspekty a provozní úkony:

- identifikace souborů k zálohování;
- určení stáří zálohovaných souborů;
- určení závislostí mezi systémy;
- určení množiny offline záloh;
- uplatnění pravidla 3-2-1;
- určení vhodného technického přístupu k vytváření záloh.

1. Identifikace souborů k zálohování

Soubory se prioritizují na základě klasifikace. Příklady důležitých souborů jsou:

- obrazy serverů pro jejich obnovu;
- logy;
- soubory uživatelů;
- aplikační data.

2. Určení stáří zálohovaných souborů

Určení maximálního stáří zálohy má za cíl obnovení systému s minimalizací inkonzistence (ztráty dat, která již nejsou součástí zálohy). Jinými slovy, jak často provádět rozdílové zálohy. Pojem – Recovery Point Objective (RPO).

3. Určení závislostí mezi systémy

Určení závislostí mezi systémy má pomoci správně určit požadavky pro pořadí obnovování. Tedy zkrátit dobu pro obnovení služby. Pojem – Recovery Time Objective (RTO).

4. Určení množiny offline záloh

Offline zálohy musí rovněž splňovat všechny pravidla zálohování, jako je doba obnovy nebo stáří záloh. Offline zálohy mohou obsahovat citlivé údaje, jakými jsou např. logy, hesla nebo digitální certifikáty.

5. Uplatnění pravidla 3-2-1

Pro zvýšení šance obnovení ztracených nebo poškozených dat, se uplatňuje pravidlo 3-2-1:

- 3 - jsou pořizovány tři kopie každého důležitého souboru: jedna primární a dvě záložní;
- 2 - jsou pořizovány dané kopie na dvou typech úložných médií jako prevence proti různým typům hrozeb;
- 1 - je pořizována jedna kopie “offsite”.

6. Určení vhodného technického přístupu k vytváření záloh

V rámci technického přístupu organizace je rozlišováno:

- jak jsou zálohy tvořeny (automatizovaně nebo manuálně);
- s využitím agenta nebo bez;
- úložiště záloh (v cloudu, na lokálním HDD, na diskovém poli nebo na odnímatelných médiích);
- jaké zálohy se budou šifrovat;
- a jaký typ záloh se bude vytvářet (přírůstkový nebo celý).

7. Určení možností při relokaci pracoviště

Ne všechny zálohovací možnosti jsou přenositelné. Požár, povodeň, nebo jiné katastrofické události mohou vyžadovat dočasné nebo trvalé přemístění. Na Offsite zálohách nebo zálohách na přenositelných médiích musí být použitelná data pro krizové zprovoznění primárních aktiv.

8. Identifikace regulačních a právních požadavků

Regulační a právní požadavky na uchovávání dat mohou ovlivnit zálohovací plán a používaný technický přístup. Zároveň je nutné identifikovat a splnit specifické požadavky na retenci dat. V obou případech je nutné se ujistit, že jsou dodržovány.

c) Pravidla a postupy dlouhodobého ukládání

S dlouhodobým ukládáním souvisí archivování. Zatím co pro zálohování a archivování mohou být použité rozdílné techniky, je mezi nimi úzký vztah. Archivování zahrnuje vytváření a uchovávání kopií záloh pro dlouhodobé uložení. Archivní záloha musí splňovat podmínku čitelnosti minimálně 10 let a být ve shodě se Spisovým a skartačním

řádem. Prostor pro uložení archivních záloh musí splňovat požadavky bezpečného prostředí, fyzického zabezpečení a kontroly přístupu osob.

Dlouhodobý archiv musí být oddělen od produkčních systémů.

d) Pravidla bezpečného zálohování a dlouhodobého ukládání informací

Šifrování je doporučeno pro neaktivní data (data-at-rest) a data v přenosu (data-in-transit), za účelem zabránění zveřejnění dat. Za neaktivní data lze přitom považovat data uložená a skladovaná v trvalém úložišti. Šifrovací možnosti zahrnují šifrování disků, šifrování souborů, a šifrování pomocí TLS a HTTPS. Šifrování vede k závislostem, jakými je například správa šifrovacích klíčů.

e) Pravidla a postupy obnovy

Obnova dlouhodobě archivovaných dat se primárně provádí do izolovaného prostředí (nebo air-gapped prostředí), po kontrole konzistence dat sekundárně do obnovovaného stroje nebo aplikace.

Součástí klasifikace dat je určení předpokládané doby obnovy dat ze zálohy, což má za cíl minimalizovat negativní dopady na chod organizace a stanovit dobu obnovy aktiva.

Je potřeba vzít v úvahu omezení, která by mohla ovlivnit dobu obnovy, např. šířka přenosového pásma, HW prostředky atp.

Pro systémy založené na transakcích, jakými jsou například databáze, je potřebné implementovat obnovení transakcí, jakými jsou např. rollback transakcí, redo logy, online přírůstkové zálohy.

f) Pravidla a postupy testování zálohování a obnovy

Testování obnovy ze záloh by mělo být plánováno a vykonáváno s frekvencí, která dává pro organizaci smysl, např. každého půl roku. U VVŠ obvykle před novým semestrem. Za testování obnovitelnosti dat je považováno i vynucená obnova dat.

Výsledky testování jsou uvedeny v záznamech a jsou podle nich upraveny předpokládané časy obnovy dat.

Pokud je to aplikovatelné, na základě výsledků testů by měly být vyvinuty tzv. “Lessons learned”.

g) Politika přístupu k zálohám, ukládaným informacím

Přístupová práva k dlouhodobým archivům musí být oddělená od přístupových práv k administraci provozního úložiště a záloh.

Jsou používány separátní uživatelské účty a přístupové údaje.

Při pokusu o smazání dlouhodobých archivů je vyžadována úspěšná duální autorizace a záznam. Duální autorizace zajišťuje, že operace smazání bude pod dohledem dvou kvalifikovaných pracovníků. Organizace může zvážit rotaci duálních autorizačních práv napříč jinými osobami, v rámci snížení rizika ztráty archivních dat.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.