Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-020**
Název dokumentu:	**Politika bezpečného používání kryptografické ochrany**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Působnost bezpečnostní politiky se vztahuje na všechny uživatele, veškerou komunikaci a citlivé informace, ve vztahu ke všem datům a informacím dle jejich klasifikace.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 18, 19, 26
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	3 + 1
Verze:	1.1
Význam a benefity:	Kryptografie zajišťuje v kybernetické bezpečnosti důvěrnost v oblasti digitální komunikace.
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

Efektivita kryptografických služeb závisí na kvalitě komplexu všech faktorů zejména na

- síle algoritmu,
- řízení přístupů,
- rozličných fyzických prvcích (omezení přístupu ke klíčovému hardwaru, odolnosti hardwaru proti nabourání a
- dlouhodobé správné správě klíčů.

Správa kryptografických klíčů je soubor technik a postupů, které umožňují vytváření a udržování vztahů mezi jednotlivými klíči, které jsou vydávány a spravovány autorizovanými stranami.

Základním úkolem správy klíčů je starat se neustále o jejich ochranu a integritu v průběhu celého řízeného životního cyklu klíče, který zahrnuje procesy

- generování,
- uchování,
- sdílení
- likvidace a
- náhrada jiným.

Klíče jsou vydávány, pokud je to možné, jen pro jeden předepsaný způsob využití, tedy přístupu k

- šifrování jiných klíčů,
- šifrování dat atd.

a není možné je použít k jiným účelům. Vícenásobné používání jednoho klíče vede k oslabení systému.

a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu

Kvalita klíče a šifrování (aktuální odolnost) je základním předpokladem pro udržení důvěrnosti komunikace. Jelikož se kryptografie i úspěšné útoky vyvíjí, aktualizuje NÚKIB[1] platná doporučení kryptografické ochrany v oblastech:

- Symetrické algoritmy
- Asymetrické algoritmy
- Algoritmy hašovacích funkcí
- Algoritmy pro bezpečné ukládání hesel

Správci mají povinnost při nastavení systémů tato doporučení dodržovat, což pravidelně dokládají v záznamu kontrol.

[1] Příloha č.1: Minimální požadavky pro kryptografické algoritmy verze 4 (2025).

b) Pravidla kryptografické ochrany informací

Servery pro webové služby používají automatické přesměrování nešifrovaného připojení HTTP na šifrovanou komunikaci HTTPS (https://požadovaná_služba). Uživatelé musí používat při prohlížení služeb protokol HTTPS.

1. při přenosu po komunikačních sítích

Pro předávání informací elektronickou komunikací je od určitého stupně (interní/TLP:GREEN a výše) vyžadována vyšší míra zabezpečení komunikace pomocí kryptografických prostředků.

Nepoužití kryptografie je v takových případech považováno za porušení povinností a mlčenlivosti zaměstnance.

2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat

Ukládání kryptografických prostředků na externí nosiče uživateli je rovněž řešeno v podpůrném materiálu výše.

Pro ukládání kryptografických prostředků na externí nosiče (digitálně nebo analogově) administrátory platí stejné zásady, ve víceúrovňové hierarchii.

c) Systém správy klíčů

Politika zahrnuje všechny úrovně platných i archivovaných klíčů.

Základní pravidlo: otevřená podoba klíčů se nesmí v celém systému nikdy objevit, ledaže by byla dostatečně fyzicky chráněna. Není-li velmi významně odolná fyzická ochrana k dispozici, klíče jsou buď zašifrovány pomocí jiných klíčů, nebo alespoň rozděleny do dvou a více částí.

Bezpečnostní nastavení ochrany klíčů musí zamezit následujícím situacím, kdy případný narušitel:

- Nesmí získat otevřený text (analogový, či digitální)
- Nesmí mít přístup k systému, kde lze najít otevřený text
- Nesmí znát dešifrovací algoritmus a zároveň mít dešifrovací klíč nebo jej dokázat někde v systému nalézt nebo mít možnost jej prolomit.

Je dodržována hierarchie klíčů, které chrání jednotlivé vrstvy služeb. Hlavní klíč je nadřazen klíčům nižší úrovně, které slouží například k distribuci podřízených klíčů pro další úrovně – šifrování zabezpečené komunikace nebo k ověřování integrity dat.

Po celou dobu existence klíče probíhá monitoring jeho stavu a expirace.

Likvidace klíče:

- Fyzický klíčový materiál na papíru či podobném záznamovém prostředku je potřeba nenávratně zničit.
- Klíčový materiál na všech jiných typech záznamových prostředků musí být zničen tak, aby jej nešlo fyzicky ani elektronicky obnovit.
- Útočník nesmí mít možnost klíč zneužít ať už ze smazaného nosiče, nebo paměti.

V ostatním platí pravidla pro fyzickou likvidaci médií.

Historie revizí

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