# Jihočeská univerzita v Českých Budějovicích

| | |
|---|---|
| *Označení dokumentu:* | **ISMS-017** |
| *Název dokumentu:* | **Politika ochrany před škodlivým kódem** |
| *Typ dokumentu:* | Interní dokument – **TLP:GREEN** |
| *Rozsah*: | Vztahuje se na veškerá HW IT zařízení organizace. |
| *Prvek legislativy:* | Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 10, 21 |
| *Datum vydání:* | 07. 07. 2026 |
| *Datum účinnosti:* | **07. 07. 2026** |
| *Platnost do:* | odvolání |
| *Počet stran + příloh:* | 2 + 0 |
| *Verze:* | 1.1 |
| *Význam a benefity:* | Kontrola výskytu, pohybu a spouštění veškerých programových kódů významnou měrou omezuje skryté aktivity (útoky) a hrozby, čímž přispívá k udržení bezpečnosti (z hledisek DDI aktiv). |
| *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

JU řídí oprávnění ke spouštění kódu na koncových stanicích, mobilních zařízeních, serverech, datových úložištích a výměnných datových nosičích, komunikační sítích a prvcích komunikační sítě a obdobných zařízeních.

JU monitoruje a řídí používání a automatické spouštění obsahu výměnných zařízení a datových nosičů.

JU provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem na všech výše uvedených komponentách.

Škodlivým kódem je počítačový program, který lze charakterizovat jako např. viry, spyware, trojské koně atp.

Za provoz a aktualizaci nástrojů detekujících škodlivý kód je stanovena odpovědnost konkrétních osob.

Ochrana před škodlivým kódem je součástí pravidelného školení zaměstnanců, smluvního řízení dodavatelů a penetračních testů.

### a) Pravidla a postupy pro ochranu síťové komunikace

K ochraně sítě je určen perimetr (firewall) a to jak vnější, tak vnitřní, mezi jednotlivými VLAN. Případně mohou být nasazeny další technické prostředky pro ochranu komunikace v síti (IDS/IPS apod.). Všechny tyto prostředky jsou centrálně spravovány, je prováděna jejich pravidelná aktualizace (stahování signatur), sledování a řešení jejich zranitelností, a další úkony zajišťující jejich plnou funkčnost.

Vzdálené přístupy do vnitřní sítě jsou umožněny pouze autorizovaným uživatelům a technickým prostředkům pomocí šifrované komunikace přes VPN.

### b) Pravidla a postupy pro ochranu serverů a sdílených datových úložišť

Na všech, serverech a datových úložištích je pravidelně aktualizován operační systém a firmware, centrálně instalován a automaticky spouštěn antivirový software, je prováděna jeho pravidelná aktualizace, distribuce a vyhodnocování jeho účinnosti.

### c) Pravidla a postupy pro ochranu pracovních stanic

Na všech pracovních stanicích, přenosných a mobilních zařízeních je pravidelně aktualizován operační systém, centrálně instalován a automaticky spouštěn antivirový software, je prováděna jeho pravidelná aktualizace a vyhodnocování jeho účinnosti.

V rámci monitoringu a řízení použití externích paměťových médií připojovaných k počítači nebo výměnných médií vkládaných do počítače (flash disk, CD/DVD atp.) jsou všechna úložiště automaticky podrobena antivirové kontrole.

V rámci antivirového programu je aktivována funkce ochrany před malware/adware a jinými hrozbami spojenými s prohlížením webových stránek.

Uživatelé pracovních stanic nemají přístupová práva k administrátorskému účtu a nemohou instalovat a spouštět neautorizované aplikace a programy.

Uživatelé koncových zařízení mohou používat pouze webové prohlížeče se zajištěnou podporou a je stanoven způsob blokace automatického otevírání oken webových prohlížečů. Případné výjimky (zejména z důvodů aktualizací některých aplikací, pluginů atp.) musí být zdůvodněny a ošetřeny.

## Historie revizí

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