Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-016**
Název dokumentu:	**Politika bezpečnosti komunikační sítě**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Vztahuje se na veškerá síťová a komunikační zařízení a prostředky JU.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 18
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	2 + 0
Verze:	1.1
Význam a benefity:	Komunikační síť (infrastruktura) je velmi významným podpůrným aktivem, na kterém závisí téměř všechna ostatní IT aktiva. Proto je její ochrana pro JU klíčová.
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 zavádí a provádí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti komunikačního systému s ohledem na významný informační systém a vede o nich bezpečnostní dokumentaci.

Ochrana komunikační sítě je také součástí řízení dodavatelů. Zohlednění nezbytných požadavků na dodavatele není považováno za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku v hospodářské soutěži.

a) Pravidla a postupy pro zajištění bezpečnosti sítě

Komunikační síť musí být rozdělena (segmentována) na logické celky, aby bylo možné omezit malware a další hrozby a byla zvýšena účinnost výkonu sítě; toto dělení musí být patrné v topologii sítě.

Musí být stanoven systém řízení komunikace v rámci komunikační sítě a stanoveny bezpečnostní perimetry.

Při použití vzdáleného přístupu (bezdrátová i kabelová komunikace) musí být zaveden systém šifrování, aby nemohlo dojít k narušení důvěrnosti a integrity dat.

Musí být zavedeny nástroje a způsob detekce nežádoucích událostí, monitoringu komunikace na síti a zaveden proces pro blokování nežádoucí komunikace.

Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty musí být použit nástroj, který zajistí ochranu integrity komunikační sítě.

b) Určení práv a povinností za bezpečný provoz sítě

Musí být stanovena odpovědnost za architekturu komunikační sítě.

Musí být stanovena odpovědnost za nastavení komunikační sítě a správu aktualizací.

Musí být stanovena odpovědnost za provoz komunikační sítě.

Musí být stanovena odpovědnost za sledování, zaznamenávání a blokování nežádoucí komunikace v komunikační síti a identifikaci síťových zařízení.

Musí být stanovena odpovědnost za přidělování přístupů do komunikační sítě.

c) Pravidla a postupy pro řízení přístupů v rámci sítě

Přístup do sítí musí být minimalizován tak, aby každý zaměstnanec přistupoval pouze v rozsahu, který je nutný pro výkon jeho pracovních povinností.

Pro jednotlivé role správců sítí musí být stanoveny postupy způsobu povolování, schvalování a odebírání vzdálených přístupů, včetně přístupů k průmyslovým, řídicím a obdobným specifickým systémům.

Řízení přístupů k sítím se musí týkat i bezpečnosti průmyslových, řídicích a obdobných specifických systémů.

Rozsah a způsob přístupu zaměstnanců dodavatelů musí být stanoven smlouvou s dodavatelem.

O přidělení a odebrání práv musí být vedeny záznamy.

d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti

Vzdálený přístup do sítě musí být omezen pouze na určená zařízení a pro uživatele, kteří jej potřebují pro výkon svých odpovědností.

Vzdálený přístup do sítě musí být omezen pouze na dobu, která je nutná pro uživatele.

e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

Musí být stanoveno co, jakým způsobem (pomocí jakého nástroje), jak často monitoruje síťový provoz, kde jsou vedeny záznamy o výsledcích monitoringu a stanovená mezní akceptovatelná hodnota výsledků monitoringu.

Historie revizí

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