

PRAVIDLA KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

PBS VELKÁ BÍTEŠ

(platné od 1/2026)

Účel

Účelem těchto Pravidel kybernetické a informační bezpečnosti PBS Velká Bíteš (dále jen „Pravidla“) je stanovení pravidel kybernetické bezpečnosti, která upravují způsob externího přístupu a práce externích stran se vzdáleným nebo fyzickým přístupem do informačních systémů společnosti První brněnská strojírna Velká Bíteš, a. s. (dále jen „PBS“).

Platnost a účinnost

Tyto Pravidla jsou platná a účinná ode dne jejich vydání až do dne nabytí účinnosti jejich aktualizované verze pro všechny externí strany, které se písemně zavázaly k jejich dodržování nebo akceptovaly obchodní podmínky PBS.

Nové znění Pravidel nabývá účinnosti dnem jejich zveřejnění na webových stránkách www.pbs.cz není-li vzájemně dohodnuto jinak. Vydáním aktualizované verze pozbývá předchozí verze platnost ke dni zveřejnění nové verze. Výjimky jsou přípustné pouze po předchozím projednání a vzájemném písemném odsouhlasení.

PBS si vyhrazuje právo Pravidla kdykoli změnit či aktualizovat. Externí strana je povinna se s aktuálním zněním dokumentu seznámit.

Definice „externí strany“ – každá fyzická nebo právnická osoba stojící mimo organizační strukturu společnosti PBS, která má přístup k informačním aktivům, systémům nebo datům společnosti, např.:

- dodavatelé, případně jejich subdodavatelé;
- zákazníci, klienti, odběratelé;
- obchodní a smluvní partneři;
- externí konzultanti a auditoři;
- provozovatelé kritické infrastruktury nebo cloudu.

Použité zkratky

2FA Two-Factor Authentication
IT Informační technologie
PBS První Brněnská Společnost Velká Bíteš, a.s.

PIN Personal Identification Number
SMS Short Message Service
UTC Coordinated Universal Time
VPN Virtual Private Network

Odovědnost za dodržování Pravidel

Externí strana je odpovědná za dodržování Pravidel u svých zaměstnanců nebo subdodavatelů a zajistí pro ně dostatečné seznámení s Pravidly, jejich proškolení a včasné oznámení o případných aktualizacích.

Povinnosti externí strany

Externí strana je povinna zajistit ochranu vlastní infrastruktury a procesů.

Externí strana je povinna okamžitě oznámit změny osob mající přístup do systému PBS případně osob, která mají umožněný vstup do prostor PBS.

Externí strana se zavázala schválením těchto Pravidel k dodržování následujících pravidel:

Účty a hesla

- přihlašovací údaje poskytnuté PBS nesmí být s nikým sdíleny;
- přihlašovací údaje nesmí být zaznamenány na jednoduše viditelném místě (papír, deník, vybavení atd.), do lehce čitelných souborů, internetových prohlížečů či na přenosná média a je doporučeno využívat nástroje pro správu hesel;
- je povinen vždy unikátně vytvořit heslo, tj. nepoužívá stejné heslo pro více účtů ani nepoužívá stejná hesla pro soukromé účely;
- Heslo splňuje min. 3 ze 4 podmínky:
 - malé písmeno
 - velké písmeno
 - číslice
 - speciální symbol

a má minimální délku s ohledem k účelu využití účtu:

- běžný účet – 12 znaků
- privilegovaný účet – 17 znaků
- účet pro servisní běh – 22 znaků

Internet

Externí strana nepřistupuje při výkonu činnosti u PBS na webové stránky, které nepotřebuje ke své činnosti.

Externí strana nevyužívá veřejná či soukromá uložení v internetu (Google disk, Dropbox, OneDrive, domácí NAS atd.) pro data PBS.

Koncové zařízení externí strany

Externí strana je povinna zajistit, aby zařízení používané pro výkon činnosti splňovalo následující požadavky:

- Připojení probíhá výhradně ze zabezpečené sítě (např. firemní nebo důvěryhodná domácí síť, síť telekomunikačního operátora);
- Operační systém, webový prohlížeč a další používané aplikace mají:
 - aplikované aktuální bezpečnostní záplaty,
 - aktivní a aktualizované bezpečnostní mechanismy (např. antivirus);
- Externí strana nesmí umožnit přístup třetím osobám a je odpovědná za ochranu svých přístupových údajů;
- Disky musí být šifrovány;
- Při přenosu dat musí být veškeré informace šifrovány jak v klidu, tak i během přenosu.

Vzdálený přístup

Vzdálený přístup externí strany je realizován prostřednictvím VPN klienta CheckPoint nainstalovaného na koncovém zařízení externí strany. Autentizace probíhá pomocí uživatelského certifikátu, PINu a dvoufaktorového ověření formou SMS.

Po úspěšné autentizaci se externí strana dostává na perimetr sítě PBS a přihlašuje se na Windows terminálový server pomocí doménového účtu, kde probíhá činnost externí strany. Terminálový server má nainstalovaný software pro záznam uživatelských relací.

Tento způsob přístupu nevyžaduje pořízení softwaru nebo licence a externí straně nevznikají žádné další náklady spojené s dodržováním požadovaných Pravidel.

Výjimečné způsoby připojení

Ve výjimečných případech, kdy není možné:

- a) připojení přes vzdálenou plochu na terminálový server, je možné povolit přímé připojení z VPN klienta na konkrétní koncové zařízení v síti PBS;
- b) připojení pomocí VPN klienta, je možné zřídit Site-to-Site VPN řešení.

Tyto výjimky musí být předem schváleny oddělením IT / kybernetické bezpečnosti PBS, jsou časově omezené a podléhají evidenci a pravidelnému přehodnocení.

Zřízení vzdáleného přístupu

O zřízení vzdáleného přístupu žádá odpovědná osoba ze strany PBS, která je za spolupráci s externí stranou odpovědná. Na základě schválené písemné žádosti je externí straně vytvořen vzdálený přístup a jsou mu předány přístupové údaje a pokyny. Jednotlivá žádost o vzdálený přístup je na dobu určitou dle délky plánované spolupráce nebo maximálně na jeden rok.

Revize a ukončení vzdáleného přístupu

- Vzdálené přístupy jsou minimálně jednou ročně revidovány ve spolupráci s odpovědnou osobou PBS za účelem ověření, zda je přístup stále oprávněný a potřebný.
- Při ukončení spolupráce s externí stranou nebo při zániku důvodu přístupu, je odpovědná osoba PBS povinna neprodleně zajistit ukončení všech přístupů externí strany k systémům PBS.
- Externí strana je povinna po ukončení spolupráce:
 - a) ukončit používání všech přístupových údajů a
 - b) odstranit veškerá data PBS ze svých zařízení, pokud nebylo dohodnuto jinak.

Výkon činnosti

Externí strana se k systémům PBS standardně připojuje pouze v čase 7:00 – 17:00 (UTC+1) v pracovních dnech.

V případě potřeby připojení mimo toto časové rozmezí je externí strana povinna:

- požádat o schválení odpovědnou osobu PBS, nebo
- případně získat souhlas oddělení IT / kybernetické bezpečnosti PBS.

Nakládání s daty a informacemi

Externí strana je povinna data PBS používat výhradně za účelem plnění smluvních povinností.

Kopírování, ukládání nebo přenos dat PBS mimo infrastrukturu PBS je povoleno pouze s předchozím souhlasem PBS.

Ukládání dat PBS do veřejných nebo soukromých cloudových služeb třetích stran je zakázáno, pokud není výslovně schváleno PBS.

Přenosná média musí být šifrována a evidována.

Fyzický přístup a připojení

Externí strana je oprávněna se v prostorách PBS pohybovat pouze se souhlasem odpovědné osoby PBS a pouze v rozsahu nezbytném pro výkon své činnosti a zavazuje se dodržovat Pravidla pro vstup, vjezd a působení externích osob v areálu PBS.

Připojení vlastních zařízení externí strany k síti PBS (LAN, Wi-Fi, USB, sériová rozhraní apod.) je povoleno pouze se souhlasem oddělení IT / kybernetické bezpečnosti PBS.

Je zakázáno:

- připojování neautorizovaných zařízení do síťových zásuvek PBS;
- připojování vlastních datových nosičů bez předchozího schválení;
- obcházení fyzických nebo technických bezpečnostních opatření.

Jakékoli servisní zásahy do infrastruktury PBS (servery, síťové prvky, koncová zařízení) mohou být prováděny pouze na základě schváleného požadavku a v přítomnosti nebo se souhlasem odpovědné osoby PBS.

Bezpečnostní událost a incident

V případě podezření, že došlo ke ztrátě, odcizení nebo kompromitaci zařízení či přístupových údajů, je externí strana povinná tuto skutečnost neprodleně oznámit odpovědné osobě PBS a Manažerovy kybernetické bezpečnosti (isms@pbs.cz), nebo přes web www.pbs.cz.

Externí strana je povinná poskytnout nezbytnou součinnost při řešení bezpečnostní události nebo incidentu.

PBS je oprávněna dočasně nebo trvale zablokovat přístup externí stran po dobu nutnou k vyšetření situace.

Ostatní

PBS má právo provádět bezpečnostní audit externí strany. Externí strana je povinná poskytnout nezbytnou součinnost.

PBS má právo bez jakéhokoliv předchozího upozornění odebrat přístupové oprávnění do sítě a systému, a to včetně i VPN přístupu, pouze z důvodu podezření na porušení podmínek uvedených v tomto dokumentu nebo při podezření na bezpečnostní incident. Tato akce může být prováděna i automaticky (systémem).

V případě porušení těchto Pravidel je PBS oprávněna požadovat náhradu veškeré škody, která jí vzniknou v důsledku takového porušení.