synlab czech s.r.o. · Sokolovská 100/94 · Karlín · 186 00 Praha 8

Bezpečnostní politika společnosti synlab czech s.r.o.

Platnost dokumentu:	**4. března 2021**
Datum vypracování:	22. února 2021
Datum schválení:	3. března 2021
Vypracoval:	Ing. Markéta Svatošová, Ing. Michaela Štrbíková
Schválil:	Ing. Kateřina Bílly Danyšová, generální ředitelka
Garant dokumentu:	Ing. Markéta Svatošová, manažerka bezpečnosti informací
Verze:	**07**
Identifikace dokumentu:	**VD 06**
Důvěrnost:	**Veřejné**
Výtisk č.:	
Ostatní informace:	Nahrazuje verzi 06, platnou od 27.11.2019.

Vedení společnosti synlab czech s.r.o. si uvědomuje, že vysoká úroveň využívání informačních systémů, jak v rámci zpracování klinických materiálů v laboratořích, tak při komunikaci s dodavateli a zákazníky, přináší nemalá rizika. Bezpečnostní politika společnosti synlab czech s.r.o. je základním dokumentem, který vedení společnosti vydává pro zajištění bezpečného a efektivního provozu informačních a komunikačních systémů zejména k zabezpečení ochrany osobních údajů.

Účelem bezpečnostní politiky je formulace jasné a závazné koncepce řešení bezpečnosti informací a definice základních přístupů při budování bezpečnosti informací společnosti synlab czech s.r.o. Hlavními procesy společnosti je laboratorní a ambulantní činnost, při které společnost vystupuje jako správce a zpracovatel osobních údajů a citlivých osobních údajů (dále jen „osobní údaje“) pacientů dle zákona č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Dále společnost zpracovává osobní údaje zaměstnanců a třetích stran, které jsou vedeny v elektronické i tištěné podobě.

Z tohoto důvodu jsou vytvořeny 4 základní oblasti bezpečnostní politiky:

- I. Pravidla pro všechny uživatele IT
- II. Pravidla pro řízení provozních aktiv v oblasti IT
- III. Pravidla pro správu aplikací
- IV. Soukromí a ochrana osobních údajů

Bezpečnostní politika vytváří základ pro tvorbu interních norem – bezpečnostních zásad a postupů, bezpečnostních standardů, směrnic a definuje zásady chování všech zaměstnanců i třetích stran při využívání informačních a telekomunikačních technologií.

Vedení společnosti deklaruje bezpečnostní politikou svou strategii trvalého zajišťování informační bezpečnosti a ochrany osobních údajů jako nedílné součásti všech řídicích procesů.

K prosazování bezpečnostní politiky a politiky ochrany osobních údajů skupiny SYNLAB Group je ve společnosti zaveden a rozvíjen systém managementu bezpečnosti informací vycházející z GDPR.

Bezpečnostní politika je formulována v následujících bodech:

I. Pravidla pro všechny uživatele IT

(tj. všichni zaměstnanci, smluvní zaměstnanci a konzultanti)

Všichni uživatelé informačních technologií (dále jen „IT“) zpracovávají ve společnosti synlab czech s.r.o. informace a osobní údaje v elektronické podobě prostřednictvím jednotlivých aplikací. Tyto informace zadávají, ukládají, mění, zálohují za použití IT. Z tohoto důvodu jsou stanoveny tyto dílčí bezpečnostní politiky:

➢ Incident Management

Jakékoliv narušení nebo pokusy o narušení bezpečnosti informací a osobních údajů a všechny zjištěné bezpečnostní nedostatky v IT systémech, musí být oznámeny manažeru bezpečnosti informací.

E-mailová adresa pro témata týkající se IT bezpečnosti je **it-security@synlab.cz**.

Na všechna ohlášení narušení bezpečnosti informací a zabezpečení osobních údajů nebo nedostatků následuje rychlá reakce, a je přijato opatření zabraňující možnosti opakování těchto situací v souladu s interním dokumentem PI.ISMS 01 Bezpečnostní incidenty.

➢ Přípustné využití

Autorizovaní uživatelé IT systémů musí dodržovat zásady bezpečného používání těchto systémů a aktiv.

Uživatel musí dodržovat přijatá organizačně-technická opatření a zajistit bezpečnost informací o ochranu osobních údajů ve fyzické a logické formě a chránit informace a osobní údaje před neoprávněným přístupem a vyzrazením.

➢ IT Outsourcing

Proces výběru dodavatele musí být dodržován, přičemž každý externí dodavatel služeb týkajících se IT služeb a produktů, musí splňovat veškeré bezpečnostní požadavky a je pravidelně hodnocen a přezkoumáván, viz QS 31 Výběr a hodnocení dodavatelů.

Přístupová práva do aplikací společnosti jsou zástupcům dodavatelů přidělována pouze po schválení manažera IT a člena vedení společnosti, a to v rozsahu nezbytném pro plnění předmětu smlouvy dle interního dokumentu PI.ISMS 04 Řízení přístupových práv.

➢ Zadávání veřejných zakázek v oblasti IT

Zadávání veřejných zakázek v oblasti IT se řídí procesem výběru dodavatelů v souladu se zákonem č.134/2016 Sb. o zadávání veřejných zakázek.

Bezpečnostní požadavky na hardware, software a služby, které jsou předmětem veřejné zakázky, musí být označeny a zahrnuty do specifikace požadavků.

➢ Management smluv o úrovni poskytovaných služeb

Úroveň služeb v oblasti IT je dohodnuta, monitorována, zaznamenávána a porovnávána s definovanými požadavky.

➢ Přístup třetích stran

Přístup třetí strany k IT systémům je nastavený na bázi toho, co je nutné vědět a s příslušnými autorizacemi. Jedná se o smluvní partnery definované v interní dokumentaci.

Se třetími stranami musí být podepsány dohody o zajištění bezpečnosti informací zachování důvěrnosti, které chrání společnost před neoprávněným přístupem a modifikací IT systémů.

Před zpřístupněním osobních údajů třetím stranám, které zpracovávají osobní údaje musí být prostřednictvím smluvních ujednání zajištěno zavedení technicko-organizačních opatření, která chrání osobní data před bezpečnostním incidentem, jako je ztráta, zpřístupnění nebo zneužití.

➢ Personální zabezpečení

Zaměstnanci s přístupem k IT systémům si musí být vědomi své odpovědnosti za zachování bezpečnosti informačních systémů a zabezpečení ochrany osobních údajů.

Uživatelská přístupová práva do jednotlivých aplikací jsou poskytována oddělením IT na základě pracovních povinností a zrušena nebo změněna společně se změnami pracovního zařazení v součinnosti s personálním oddělením.

➢ Segregace povinností

Povinnosti a oblasti odpovědnosti je nutné rozdělit ve snaze snížit možnost neoprávněných úprav, zneužití IT systémů nebo zpřístupnění osobních údajů neoprávněným osobám.

II. Pravidla pro řízení provozních aktiv v oblasti IT

IT infrastruktura je nezbytnou součástí chodu společnosti a musí splňovat vysoké nároky na bezpečnost a dostupnost. Proto byly stanoveny bezpečnostní politiky, které zajišťují vysokou bezpečnost dat včetně osobních dat, jak z pohledu jejich zneužití, tak z pohledu integrity a kontinuity. Je zajištěn řízený přístup k nim a tam kde je to potřebné, jsou data krytována. Celý systém musí být monitorován a řízení jeho změn a kontinuita zachovány.

Z těchto důvodů jsou stanoveny následující dílčí bezpečnostní politiky:

➢ Správa datových center

U datových center je zajištěna přiměřená fyzická a logická ochrana.

Nezbytný oprávněný přístup do datového centra je zajištěn pro správce IT.

➢ Bezpečnost sítě

Nezbytný přístup do sítě společnosti synlab czech s.r.o. je poskytován po příslušné autorizaci.

Je nezbytné implementovat politiku silných hesel a autentizační postupy, viz PI.ISMS 02 Používání přístupových hesel.

Uživatelé jsou jedinečně identifikovatelní.

➢ Řízení aktiv

Fyzická aktiva jsou vedena v inventárním soupisu.

IT systémy jsou klasifikovány, označeny a musí s nimi být manipulováno s opatrností odpovídající jejich citlivosti.

➢ Fyzické zabezpečení

Na všech pracovištích společnosti je zabráněno neoprávněnému fyzickému přístupu k majetku společnosti synlab czech s.r.o. Ochranu majetku pomáhá zabezpečit kamerový systém, pravidla jeho provozování popisuje pracovní instrukce PI.ISMS 07 Kamerový systém.

Pohyb aktiv je kontrolován a prováděn s řádným povolením.

➢ Kryptografické kontroly

Kde je to zapotřebí, je použito šifrování k ochraně důvěrných a striktně důvěrných informací společnosti.

Zabezpečené postupy jsou použity pro generování klíčů, jejich distribuci, zrušení a skladování v souladu s interním dokumentem PI.ISMS 05 Kryptografie.

➢ Firewall

Přístup na a z externích sítí je kontrolován a zabezpečen pomocí odpovídající brány firewall a podobných metod.

Přístup přes bránu firewall, je sledován a kontrolován.

➢ Zálohování

Kritická data jsou zálohována a pravidelně testována z hlediska obnovy. Pravidla pro zálohování dat jsou popsána v interním předpisu QS 36 Zálohování dat.

Zálohovaná data a média jsou bezpečně udržována a skladována.

➢ Monitorování

Přístup k zásadním aplikacím a síti společnosti je sledován proti podezřelé činnosti nebo narušení bezpečnosti.

➢ Antivirový systém

Vhodných nástrojů a metod je využito pro zajištění ochrany IT majetku společnosti synlab czech s.r.o.

Antivirový software a nasazené procesy zajišťuje detekci, účinné zadržení a zničení škodlivého kódu v síti společnosti. Antivirový systém je centrálně spravován a aktualizován, aby se zabránilo novým hrozbám.

➢ Řízení změn

Změny v oblasti IT aktiv včetně aplikací, serverů a síťových zařízení jsou provedeny kontrolovaným způsobem a po řádném schválení.

Pomocí pravidelného ověřování je kontrolována účinnost těchto kontrol.

➢ Plán kontinuity v oblasti IT

Pro IT systémy s kritickou hodnotou je naplánována kontinuita.

Písemný kontinuální plán pro tyto kritické systémy je udržován, testován a aktualizován oddělením IT.

➢ Management rizik v oblasti IT

Společnost identifikuje, analyzuje a zmírňuje rizika, která mají vliv na důvěrnost, integritu a dostupnost aktiv IT systémů.

➢ Práce na dálku

Vzdáleně pracovat v síti společnosti je umožněno pouze vybraných pracovníkům dle typu pracovní pozice a výhradně formou VPN.

Výjimkou jsou pracovníci podpory IT, kteří ke své práci mohou využívat aplikaci TeamViewer.

VPN je možné používat výhradně na zařízeních společnosti i BYOD. Pravidla pro práci na dálku jsou popsána v interním předpisu PI.ISMS 03 Práce na dálku.

➢ Mobilní zařízení

Mobilní zařízení používaná pracovníky společnosti jsou schválena k používání vedením společnosti a podléhají pravidelné servisní kontrole (výjimkou jsou BYOD) a jsou chráněna proti neoprávněnému přístupu pomocí hesla, PIN či jiného systému. Pravidla pro práci s mobilními zařízeními jsou popsána v interním předpisu PI.ISMS 03 Práce na dálku.

➢ Internetová úložiště

Z cloudových úložišť je povolen pouze OneDrive pro firmy, a to s firemním office365 účtem (doména @synlab.cz nebo @synlab.com). Ukládání firemních dokumentů na ostatní veřejné cloudy je striktně zakázáno.

➢ Řízení přístupu

Účelem řízení přístupu k informacím, osobním údajům a prostředkům informačních systémů společnosti je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup k těmto informacím a osobním údajům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv.

Bezpečnostním cílem je zajištění řízení přístupu realizací opatření v následujících oblastech:

a) správa přístupu uživatelů a odpovědnost uživatelů – systém správy přístupu zajistí definovaný postup přidělování, změny a odebírání přístupu, správu hesel a kontrolu přístupových práv;

b) mobilní výpočetní prostředky a práce na dálku – zvláštní pozornost musí být věnována mobilním výpočetním prostředkům a prostředkům umožňujícím práci na dálku, aby bylo zabráněno jejich zneužití.

Privilegované přístupy mají administrátoři a správci informačních systémů.

➢ Přístup dodavatelů k aktivům

Přístup k aktivům společnosti mají pouze dodavatelé vybraní a periodicky hodnocení dle interních pravidel. S těmito dodavateli jsou uzavřeny písemné smlouvy. Rizika plynoucí ze vztahů s dodavateli jsou identifikována a vyhodnocována v rámci managementu rizik ISMS.

III. Pravidla pro správu aplikací

Ve společnosti jsou instalovány komerční a zakázkové informační systémy. Na tvorbě, testování a spuštění zakázkových informačních systémů se přímo podílejí vybraní pracovníci společnosti.

Z tohoto důvodu jsou stanoveny tyto dílčí bezpečnostní politiky:

- **Licenční politika**

  Společnost respektuje zákonné normy a licenční politiku dodavatelů jednotlivých softwarů. Je povoleno používat pouze schválený software, viz PI.ISMS 11 Používání licencí.

  Uživatelé mají zakázáno instalovat si samostatně software bez předchozího schválení vedením společnosti.

- **Vývoj softwaru**

  Veškerý software vyvinutý nebo přizpůsobený pro použití ve společnosti musí odpovídat standardnímu procesu vývoje a musí zajistit, aby byly splněny požadavky na IT bezpečnost.

  Při vývoji zakázkových systémů spolupracuje společnost s dodavatelem, zadává požadavky a vytváří závazné specifikace, dle kterých je systém naprogramován.

  Testování zakázkového systému probíhá vždy ve vývojovém prostředí, a to ve dvou krocích:

  1. Nejprve testuje systém dodavatel dle harmonogramu testování.
  2. Následně uvolní verzi k testování zadavateli.

  Výjimkou v rámci dvoukrokového testování jsou opravy chyb (patche a hotpatche).

  Pouze řádně otestované zakázkové systémy jsou implementovány do produkčního prostředí.

- **Bezpečnost aplikací**

  Aplikace provozované ve společnosti mají ovládací prvky pro bezpečný vstup, zpracování, skladování a výstup dat.

  Aplikace jsou testovány na bezpečnost před nasazením.

  Přístup k aplikacím je omezen na oprávněné osoby a poskytnutá práva jsou stanovena na principu minimálních privilegií.

  Uživatelé jsou jedinečně identifikovatelní.

- **Správa konfigurace**

  IT systémy jsou nakonfigurovány pro bezpečnost a jejich konfigurace jsou zdokumentovány a zajištěny.

- **Zabezpečení operačního systému**

  Uživatelský přístup k operačnímu systému je omezen a monitorován.

  Operační systém je aktualizovaný pomocí nově vydaných bezpečnostních balíčků.

- **Zabezpečení databáze**

  Databázové systémy jsou nainstalovány, konfigurovány a spravovány podle přísných bezpečnostních norem.

  Uživatelský přístup do databáze je poskytnutý pouze po předchozí autorizaci a ověření, na bázi nezbytného minima.

IV. Soukromí a ochrana osobních údajů

Všichni zaměstnanci, smluvní zaměstnanci a konzultanti jsou povinni nakládat s osobními údaji pouze za účelem plnění pracovních povinností a v souladu s povinnostmi stanovenými zákonem, a to pouze společností určenými prostředky.

Jsou povinni chránit osobní údaje před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů. Je zakázáno osobní údaje zpřístupňovat třetím osobám (mimo pověřeným osobám). To je důležité zejména ve vztahu k osobním

údajům o pacientech a zaměstnancích, ale také k osobním údajům týkajících zákazníků, dodavatelů a obchodních partnerů a dalších osob.

- **Ochrana údajů o zaměstnancích**

  Veškeré záznamy o zaměstnancích jsou vedeny na personálním oddělení nebo vedoucím pracovníkem v uzamčeném prostoru v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů a s GDPR.

- **Ochrana údajů o pacientech**

  Údaje o pacientech jsou v elektronické podobě uchovávány v aplikacích s chráněným přístupem a pravidelně zálohovány.

  Údaje o pacientech vedené v tištěné podobě jsou uloženy v archivu nebo příručních registraturách s omezeným přístupem pro třetí strany.

- **Ochrana údajů o třetích stranách**

  Údaje zákazníků, dodavatelů, obchodních partnerů a jiných smluvních partnerů jakožto subjektů osobních údajů podléhají pravidlům nastavených dle platných právních předpisů.

  Prostřednictvím smluvních ujednání je zabezpečeno, aby veškeré subjekty, kterým mohou být osobní údaje zpřístupněny, respektovali právo na ochranu soukromí a byly povinny postupovat dle právních předpisů týkajících se ochrany osobních údajů, zákona č. 110/2019 Sb., o zpracování osobních údajů a GDPR.

  Dle pracovní smlouvy je zakázáno sdělovat třetím osobám specifické informace o pacientech, které by bylo možné zneužít pro neoprávněný přístup k datům pacientů.

  Osobní údaje a citlivé osobní údaje upravuje rozsáhlá veřejnoprávní legislativní úprava. Mezi stěžejní zákony patří zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, zákon č. 373/2011 Sb., o specifických zdravotních službách a zákon č. 110/2019 Sb., o zpracování osobních údajů a GDPR.

S touto bezpečnostní politikou jsou seznámeni všichni pracovníci společnosti synlab czech s.r.o a je závazná pro jejich chování a jednání.