Princípy bezpečného riadenia dodávateľských vzťahov

Spoločnosť GAMO a.s. kladie dôraz na bezpečné a zodpovedné riadenie spolupráce so svojimi dodávateľmi a partnermi. V rámci svojho systému manažérstva informačnej bezpečnosti uplatňuje pravidlá, ktoré zabezpečujú ochranu informácií, riadenie prístupov a bezpečný prenos dát pri poskytovaní služieb, vrátane oblastí ako cloudové riešenia, outsourcing či prevádzka informačných systémov.

Súčasťou týchto pravidiel sú aj požiadavky v oblasti bezpečnosti a ochrany zdravia pri práci, ochrany pred požiarmi a environmentu.
GAMO a.s. vyžaduje od svojich dodávateľov dodržiavanie legislatívy, zodpovedný prístup k riadeniu rizík a zabezpečenie bezpečného a environmentálne udržateľného výkonu ich činností. Cieľom je zabezpečiť, aby všetky poskytované služby boli realizované bezpečne, spoľahlivo a v súlade s požiadavkami zákazníkov aj platných predpisov.

Na tento dokument sa vzťahujú nasledujúce pojmy a symboly:

Dodávateľ	externá spoločnosť, resp. jej zamestnanci vrátane subdodávateľov vykonávajúci v spoločnosti GAMO a.s. práce akéhokoľvek druhu v súlade s dohodnutými podmienkami a okolnosťami.
Tretia strana	dodávateľ činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov GAMO a.s. ako prevádzkovateľa základnej služby v zmysle zákona 69/2018 Z.z. o kybernetickej bezpečnosti
Oprávnené osoby	osoby, ktorým GAMO a.s. alebo dodávateľ povolil vstup do infraštruktúry GAMO a.s., alebo systémov u zákazníkov spravovaných GAMO a.s., oprávnené osoby sú si vedomé potenciálnych nebezpečenstiev, bezpečnostných opatrení, ktoré treba prijať, a majú požadované certifikáty a licencie podľa regulačných požiadaviek
Manažér informačnej bezpečnosti	osoba, ktorá je na základe odbornej prípravy, vzdelania a skúseností oboznámená s platnými normami, schopná identifikovať nebezpečenstvá informačnej bezpečnosti týkajúce sa konkrétnej činnosti
Zodpovedná osoba dodávateľa	osoba zo strany dodávateľa zodpovedná za výkon dodávateľských prác a dodržiavanie všetkých interných pravidiel vydaných spoločnosťou GAMO a.s.

Obsah

1. Riadenie dodávateľských vzťahov IKT

1.1 Stratégia riadenia dodávateľských vzťahov

Spoločnosť GAMO a.s. si uvedomuje, že vzhľadom na svoje pôsobenie je výrazne angažovaná voči externým dodávateľom, ktorí poskytujú viaceré služby na podporu kritických procesov v oblasti prevádzky základnej služby – v sektore: Digitálna infraštruktúra - poskytovatelia služieb cloud computingu, ako aj z pohľadu Predmetu certifikácie ISO/IEC 27001:2022, a súvisiacich IT systémov. Na ochranu najdôležitejších procesov prevádzky základnej služby a systému manažérstva informačnej bezpečnosti a informačných prostriedkov pred známymi hrozbami a na zníženie celkového rizika pôsobiaceho na informačné aktíva, hodnotu značky a na prevádzku, je potrebná účinná politika a rámec opatrení, ktoré sa týkajú výberu dodávateľov, prípravy zmlúv s dodávateľmi, riadenia vzťahov s dodávateľmi a monitorovania dodržiavania platných politík a ďalších bezpečnostných požiadaviek.
Proces riadenia informačnej bezpečnosti v dodávateľských vzťahoch sa týka špecifických činností a zodpovedností.

a) primeraná opatrnosť a preverovanie budúcej dodávateľskej činnosti (due dilligence),
b) definícia zmluvných záruk,
c) monitorovanie dodržiavania zmluvných podmienok,
d) audit dodávateľov,
e) činnosti súvisiace s ukončením dodávateľského vzťahu.

Aby boli splnené kľúčové záväzky tejto smernice, v závislosti od typu dodávateľa, kontextu a charakteru príslušných dodávateľských činností, proces riadenia dodávateľov zahŕňať zástupcov z nasledujúcich oblastí:

a) príslušný vlastník procesu,
b) úsek zodpovedný za výber a schvaľovanie dodávateľov a riadenie dodávateľských vzťahov,
    a. v oblasti internej prevádzky – Vnútorný IS/Realizačný riaditeľ,
    b. za služby poskytované zákazníkom – Realizačný riaditeľ, Riaditeľ úseku Výskumu a vývoja
c) útvar zodpovedný za IT architektúru – Vnútorný IS,
d) informačná a kybernetická bezpečnosť – Rada IB.

Bez ohľadu na požiadavky na obsah zmlúv obsiahnuté v tejto smernici, každé zmluvné dojednanie s treťou stranou musí byť plne v súlade s požiadavkami § 7 Vyhlášky č. 227/2025 Z.z. v platnom znení, ako určuje kapitola 13 tejto smernice.
V organizácii sú určené pravidlá a postupy na riešenie prípadov porušenia bezpečnostnej politiky zo strany používateľov, administrátorov, ako aj osôb zastávajúcich niektorú z bezpečnostných rolí dodávateľov.
Každé porušenie zavedených bezpečnostných pravidiel v oblasti riadenia vzťahov s dodávateľmi bude riešené v súlade s pracovným poriadkom a disciplinárnymi smernicami.
Za stanovenie požadovanej úrovne kybernetickej bezpečnosti v kontexte spolupráce s dodávateľmi zodpovedajú vlastníci relevantných procesov a aktív organizácie. Zabezpečenie dodržiavania v organizácii určených bezpečnostných zásad, pravidiel a postupov v oblasti kybernetickej bezpečnosti zo strany externého dodávateľa je vždy zodpovednosťou konkrétnych osôb zaradených do bezpečnostných rolí na strane dodávateľa.

1.2 Bezpečnosť dodávateľských vzťahov

Proces riadenia bezpečnosti v dodávateľských vzťahoch je zachytený a udržiavaný v databáze *Zmluvy* dostupnej na Sharepointe GAMO a.s., pričom pre každý vzťah, ak je to relevantné, sú vedené najmä nasledujúce záznamy:

a) vlastník procesu,
b) manažér zmluvného vzťahu,
c) kontakty s manažmentom dodávateľa,
d) obchodné zmluvy s dodávateľom,
e) relevantný prvostupňový kontakt na strane dodávateľa pre prípady bezpečnostných incidentov,
f) charakter, objem a klasifikácia uložených alebo spracovaných informácií,
g) použité systémy a platformy,
h) právne a regulačné požiadavky,
i) celková kritickosť dodávateľa resp. dodávateľského vzťahu,
j) audit informačnej / kybernetickej bezpečnosti dodávateľa,
k) známe incidenty a porušenia predpisov,
l) postupy v prípade porušenia zavedených bezpečnostných pravidiel
m) známe problémy a riziká,
n) história auditu / zabezpečenia,
o) plány na odstránenie zistených nedostatkov a stav riešenia nedostatkov.

V procese riadenia bezpečnosti dodávateľov MUSÍ BYŤ vykonané počiatočné posúdenie rizika s cieľom určiť povahu, kritickosť / citlivosť a možné dopady v prípade výpadku poskytovaných služieb.
Rámec auditu budúceho dodávateľa, riadený príslušnou úrovňou rizika, BY MAL pred uzavretím zmluvy vyžadovať najmä nasledovné:

a) preskúmanie primeranej opatrnosti (due dilligence) s cieľom identifikovať a posúdiť riziká dodávateľskej činnosti a možné dôsledky výpadku poskytovaných služieb, zmluvné požiadavky, implementované opatrenia a preukázateľný záväzok dodávateľa k dodržiavaniu pravidiel informačnej a kybernetickej bezpečnosti ešte pred uzatvorením zmluvy,
b) preskúmanie fyzickej lokality dodávateľa, ak je to vhodné, s použitím príslušných certifikačných noriem, s cieľom zhodnotiť a potvrdiť primeranosť a účinnosť ich opatrení informačnej a kybernetickej bezpečnosti,
c) posúdenie zraniteľností a penetračné testy, ak je to potrebné na overenie primeranosti a účinnosti technických bezpečnostných opatrení dodávateľa.

Základný súbor bezpečnostných opatrení na strane dodávateľa MUSÍ BYŤ zdokumentovaný a dôsledne používaný pri uzatváraní zmluvy a zaručenia bezpečnosti informácií. MALI BY sa určiť a dohodnúť dodatočné kontroly na splnenie osobitných obchodných a bezpečnostných požiadaviek, ktoré sa majú zahrnúť do zmluvy.
Zmluva alebo iná vhodná právne záväzná dohoda vrátane dohodnutých opatrení na zabezpečenie informácií MUSÍ BYŤ prijatá. Každá zmluvná požiadavka, ktorú externý dodávateľ považuje za neprijateľnú, musí byť pred uzatvorením zmluvy vyhodnotená a prípadne vhodne ošetrená alebo formálne schválená.
Musí sa vytvoriť formálne zdokumentovaný proces, ktorý umožní pravidelné overovanie súladu externých dodávateľov s dohodnutými zmluvnými požiadavkami na zachovanie bezpečnosti informácií. Tento proces by mal zahŕňať prebiehajúce prevádzkové monitorovanie bezpečnostných opatrení využívajúc vopred dohodnutú metriku, ako aj pravidelné audity a nezávislé hodnotenia s cieľom poskytnúť komplexné záruky.

MUSÍ sa dohodnúť a do zmluvy zahrnúť metóda bezpečného ukončenia dodávateľského vzťahu, ktorá zahŕňa najmä:

a) definovanie vlastníctva a zodpovednosti za riadenie ukončovacích činností,
b) zrušenie fyzického a logického prístupu do priestorov a k informáciám,
c) vrátenie, prevod alebo, ak je to vhodné, zničenie aktív v dispozícii dodávateľa po ukončení zmluvného vzťahu,
d) pokrytie licenčných zmlúv a práv duševného vlastníctva,
e) preskúmanie a zdokonalenie činností súvisiacich s ukončovaním,
f) získanie príslušného hardvéru a softvéru.

MALI BY BYŤ zavedené formálne zdokumentované štandardy a postupy na získanie všetkého hardvéru a softvéru, ktoré pokrývajú najmä:

a) kritériá výberu hardvéru a softvéru,
b) posúdenie bezpečnosti hardvéru a softvéru, ktoré sa majú získať,
c) požiadavky na softvérové licencie,
d) proces kontroly a schválenia hardvéru a softvéru.

Hardvér a softvér používaný v GAMO a.s. MUSÍ BYŤ získavaný iba od schválených dodávateľov, testovaný pred nasadením a podporený vopred dohodnutými opatreniami na údržbu.
Riziko možných bezpečnostných zraniteľností hardvéru a softvéru, ktoré sa majú získať, BY SA MALO znížiť vymedzením požiadaviek na bezpečnosť, získaním nezávislých hodnotení z dôveryhodných zdrojov, určením bezpečnostných nedostatkov a zvažovaním alternatívnych metód na dosiahnutie bezpečnosti.

1.2.1 Hodnotenie dodávateľov z pohľadu kybernetickej bezpečnosti a prepojenie na riadenie rizík

Spoločnosť GAMO a.s. MUSÍ vykonávať systematické hodnotenie dodávateľov z pohľadu kybernetickej bezpečnosti ako súčasť riadenia dodávateľských vzťahov, a to:

- pred uzatvorením zmluvného vzťahu s dodávateľom (onboarding),
- pravidelne, minimálne raz ročne počas trvania zmluvného vzťahu,
- mimoriadne pri významnej zmene rozsahu služby, bezpečnostnom incidente alebo zmene rizikového profilu dodávateľa.

Hodnotenie dodávateľov sa vykonáva na základe jednotného hodnotiaceho formulára zameraného na riadenie kybernetickej bezpečnosti, technické a organizačné opatrenia, riadenie incidentov a kontinuity, súlad s legislatívou a zmluvné zabezpečenie.
Dodávatelia sú v rámci hodnotenia zaradení do kategórií podľa ich kritickosti (kritický / významný / nekritický dodávateľ) v závislosti od vplyvu na informačné aktíva, služby a kontinuitu prevádzky organizácie.
Výsledky hodnotenia dodávateľov z pohľadu kybernetickej bezpečnosti MUSIA BYŤ vyhodnotené z hľadiska dopadu na riziká organizácie.
Riziko MUSÍ BYŤ zaevidované v registri rizík, ak:

- dodávateľ kategórie kritický alebo významný nedosiahne požadovanú úroveň hodnotenia,
- sú identifikované závažné nedostatky v oblasti riadenia kybernetickej bezpečnosti, incident response alebo kontinuity,
- hodnotenie indikuje zvýšené riziko narušenia dostupnosti, dôvernosti alebo integrity informácií alebo služieb.

Riziko vyplývajúce z hodnotenia dodávateľa MUSÍ obsahovať najmä:

- identifikáciu dodávateľa a dotknutých služieb,
- opis dopadu rizika na organizáciu GAMO a.s.,
- určenie vlastníka rizika,
- existujúce a navrhované opatrenia, účinnosť existujúcich opatrení
- termín prehodnotenia rizika.

Opatrenia vyplývajúce z identifikovaných rizík môžu zahŕňať najmä:

- uloženie nápravných opatrení dodávateľovi,
- úpravu zmluvných bezpečnostných požiadaviek,
- obmedzenie rozsahu poskytovaných služieb,
- zapojenie dodávateľa do cvičení kybernetickej bezpečnosti a testovania pripravenosti,
- opakované alebo mimoriadne hodnotenie dodávateľa,
- zmenu alebo ukončenie dodávateľského vzťahu.

Stav rizík vyplývajúcich z hodnotenia dodávateľov MUSÍ BYŤ pravidelne monitorovaný a zohľadňovaný v rámci riadenia rizík, BCM a SMS.
Interný postup pre hodnotenie dodávateľov z pohľadu informačnej a kybernetickej bezpečnosti je zdokumentovaný v prílohe F-01-S-00-21 tejto smernice.

1.3 Princípy riadenia Dodávateľských vzťahov

1.3.1 Princíp fyzickej a objektovej ochrany priestorov organizácie

Priestory organizácie, v ktorých je umiestnený majetok dodávateľa a ktoré je potrebné fyzicky chrániť, sú na základe výstupov z analýzy rizík zabezpečené pred identifikovanými bezpečnostnými hrozbami. Zariadenia sú umiestnené tak, aby sa znižovali riziká vyplývajúce z hrozieb prostredia (najmä však pred technickými poruchami, vlhkosťou, výpadkami napájania, bleskom, ohňom, sabotážou alebo krádežou). Vybavenie chránených priestorov sa udržiava v súlade s dokumentovanými postupmi dodávateľov, aby sa zabezpečila nepretržitá dostupnosť týchto priestorov.

Spoločnosť vyžaduje od dodávateľov dodržiavanie pravidiel vstupu a pohybu v priestoroch, vrátane identifikácie a prístupu len do schválených zón. Dodávatelia musia rešpektovať všetky bezpečnostné opatrenia, sprievod oprávneným zamestnancom a zákaz manipulácie s majetkom organizácie bez súhlasu. Dodávatelia sú oboznámení s evakuačnými postupmi a majú povinnosť hlásiť akékoľvek incidenty alebo podozrenia.

Obchodné/Kritické procesy môžu prístupné iba určeným pracovníkom organizácie a určeným pracovníkom dodávateľov.

1.3.2 Princíp kybernetickej ochrany

GAMO a.s. zdokumentovala a zaviedla štandardizovaný proces a životný cyklus na riadenie vzťahov s dodávateľmi. V každom jednotlivom prípade definovala typ informačného prístupu, ktorý pridelí konkrétnym typom dodávateľov, tento povolený prístup monitoruje a riadi. Na to definovala minimálne požiadavky kybernetickej bezpečnosti pre každý typ informácie a konkrétny typ prístupov dohodnutých v zmluve s dodávateľom.

Prideľovanie prístupov ku IS GAMO alebo k účtom pod kontrolou organizácie rieši ***F-12-RN-05 Riadenie identít a prístupov IS GAMO*** .

Prideľovanie vzdialeného prístupu ku IS GAMO prostredníctvom VPN rieši ***F-05-RN-05 Žiadosť externého dodávateľa o pripojenie do VPN***

1.3.3 Princíp rizikovo orientovaného hodnotenia dodávateľov

Riadenie dodávateľských vzťahov v oblasti informačnej a kybernetickej bezpečnosti je založené na rizikovo orientovanom prístupe. Hodnotenie dodávateľov z pohľadu kybernetickej bezpečnosti a výsledné riziká sú integrálnou súčasťou systému riadenia rizík organizácie a vstupom do rozhodovania o bezpečnostných opatreniach, kontinuitných opatreniach a zmluvných podmienkach.

1.3.4 Princíp riadenia kybernetických bezpečnostných incidentov

GAMO a.s. definovala postupy pre riadenie kybernetických bezpečnostných incidentov spojených s prístupmi dodávateľov vrátane určenia zodpovednosti oboch strán. Pre tento účel školenia bezpečnostného povedomia pre osoby dodávateľa, ktoré sú v predmetnej veci zainteresované.

Riešenie a záznamy ku identifikovaným bezpečnostným incidentom rieši ***S-00-20 Zvládanie bezpečnostných incidentov***.

1.3.5 Princíp manipulácie so zariadeniami a informáciami

GAMO a.s. riadi požadované presuny informácií a zariadení na spracúvanie informácií, pričom počas presunu udržiava požadovanú úroveň kybernetickej bezpečnosti.

Pre tento účel GAMO a.s. vedie dokumentáciu vrátane identifikácie prvkov v správe dodávateľov - vo forme zoznamu aktív, kategorizácie sietí a informačných systémov. Správca konkrétneho informačného systému je povinný revidovať zoznam uvedených aktív v správe dodávateľa minimálne raz ročne.

Pre pracovné účely vo vzťahu k zákazníkom GAMO a.s. sú pracovníci dodávateľa povinní využívať výhradne e-mailové účty patriace GAMO a.s. Uvedená povinnosť platí pre externých pracovníkov (na základe dodávateľskej zmluvy, zmluvy o poskytovaní služieb) komunikujúcich v mene GAMO a.s.. Nie je prípustné, aby oficiálna komunikácia prebiehala prostredníctvom e-mailových účtov, ktoré nie sú pod kontrolou GAMO a.s.

S každým dodávateľom je uzavretá dohoda o mlčanlivosti.

1.3.6 Princíp riadenia prístupových práv

Všetky prístupy dodávateľa musia byť, ak je to možné a účelné, v súlade s politikou najmenších privilégií a potreby vedieť (Need to Know), umožnené iba na nevyhnutnú dobu a v prípade vhodnosti iba na čítanie.

Dodávateľ je povinný bezodkladne a okamžite požiadať organizáciu o zrušenie prístupu svojho pracovníka, ak takýto prístup už nie je potrebný.

Všetky vzdialené pripojenia do internej siete musia využívať VPN s dvojfaktorovou autentizáciou.

Všetky bezpečnostné pravidlá a požiadavky pre dodávateľa na prístup do sietí a informačných systémov organizácie sa vzťahujú aj na subdodávateľov dodávateľa.

Prideľovanie prístupov ku IS GAMO alebo k účtom pod kontrolou organizácie rieši ***F-12-RN-05 Riadenie identít a prístupov IS GAMO***.

1.3.7 Princíp riadenia personálnych zdrojov

V prípade prijatia, doplnenia, zmeny, alebo zrušenia oprávnenia prístupu zo strany dodávateľa predloží manažér zmluvného vzťahu takúto požiadavku na schválenie osobe zodpovednej za výber a schvaľovanie dodávateľov. Po schválení a definovaní popisu pozície osoba dodávateľa, zúčastnená na predmete plnenia zmluvy, podpisuje s GAMO a.s. dohodu o zachovávaní mlčanlivosti.

1.4 Akvizícia, vývoj a údržba IT aktív

Pri určovaní požiadaviek na akvizíciu, vývoj a údržbu IT aktív (akvizícia a údržba sietí a informačných systémov, vývoj informačných systémov) sa MUSÍ vykonať hodnotenie rizík s cieľom vyhodnotiť potenciálne bezpečnostné riziká súvisiace s dohodami o službách s ohľadom na konkrétne funkcie, ktoré majú byť poskytované. Rámec opatrení, ktorý je daný výsledkami predchádzajúceho hodnotenia rizika, by mal byť určujúci pre stupeň a hĺbku požadovanej zmluvnej ochrany ešte pred tým, ako sa tieto činnosti vykonajú.

- V tejto súvislosti GAMO a.s. určuje vlastníka rizika, implementuje organizačné a technické bezpečnostné opatrenia v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú a nie sú implementované spolu s odôvodnením.
- GAMO a.s. tiež analyzuje funkčný dopad a identifikované riziká, pričom pravidelne preskúmava a aktualizuje prijaté bezpečnostné opatrenia.

Zmluvy odrážajú odsúhlasené bezpečnostné opatrenia a schválenia od príslušných vlastníkov procesov ešte predtým, ako dôjde k uzatvoreniu a plneniu zmluvy. Zmluvy musia byť preskúmané všetkými príslušnými zainteresovanými stranami, schválené, odsúhlasené a podpísané oboma stranami.
Rámec opatrení by mal určovať dodávateľovi súbor štandardných prvkov a modelov, ktoré MUSIA BYŤ dôsledne začlenené do všetkých zmlúv o outsourcingu, ako určuje kapitola 9 tejto smernice.
Proces na riešenie akýchkoľvek bezpečnostných problémov alebo incidentov prostredníctvom dohodnutého kontaktného miesta poskytovateľa služieb outsourcingu MUSÍ existovať a MUSÍ byť formálne zdokumentovaný.
Akvizícia, vývoj a údržba IT aktív MUSÍ byť uskutočnená s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.
Akvizícia IT aktív sa uskutočňuje podľa plánovania založeného na koncepcii rozvoja aktív organizácie.
Súčasťou životného cyklu aktív organizácie je aj stanovenie bezpečnostných potrieb, bezpečnostných požiadaviek a bezpečnostných opatrení v závislosti od platnej bezpečnostnej politiky kybernetickej bezpečnosti, zásad a požiadaviek vlastníkov aktív.
Pri akvizícii jednotlivých aktív sa postupuje podľa zásad SDLC - System Development Life Cycle.

V procese vývoja informačných systémov MUSÍ byť implementovaný formálny a zdokumentovaný proces pri riadení bezpečného vývoja, kedy GAMO a.s. zohľadňuje bezpečnosť svojho vývojového prostredia, bezpečnosť pri metodike vývoja softvéru a procesy pre bezpečné kódovanie, bezpečnostné požiadavky v rámci riadenia projektu a verzií (jednotlivé fázy vrátane dizajnu, kontrolné body, spôsoby uloženia na dátových úložiskách), ako aj postupy vývojárov pri práci s identifikovanými zraniteľnosťami.
Pre testované informačné systémy, aktualizácie a nové verzie MUSIA byť vytvorené procesy akceptačného testovania s príslušnými postupmi, spôsobmi a úrovňami overovania, s určením konkrétnych zodpovedností. Rovnako MUSIA byť definované postupy na posúdenie bezpečnosti definovaných sietí a informačných systémov, hodnotenie zraniteľností a penetračné testy. Testovacie údaje MUSIA byť riadené a chránené.

1.5 Outsourcing

Spôsob výberu poskytovateľov outsourcingových služieb a prípadný prenos vybraných činnosti k nim, s dokumentovanými dohodami, ktoré budú špecifikovať požiadavky na bezpečnosť informácií MUSÍ byť implementovaný, formálny a zdokumentovaný proces, ktorým je riadený.
Zodpovednosti všetkých strán za dohodnutú úroveň bezpečnosti MUSIA BYŤ opísané v počiatočných návrhoch a výsledných zmluvách a dohodách (napríklad Zmluva o poskytovaní služieb, Rámcové zmluvy o spolupráci, Zmluvy o dielo, Rozvojové zmluvy a pod), ktoré obsahujú zmluvné dojednania o úrovni služieb (SLA – Service Level Agreement). V rámci procesu preskúmania zmlúv je potrebné vždy skontrolovať zahrnutie príslušných bezpečnostných požiadaviek.
Pri určovaní požiadaviek na outsourcing sa MUSÍ vykonať hodnotenie rizík s cieľom vyhodnotiť potenciálne bezpečnostné riziká súvisiace s dohodami o outsourcingu s ohľadom na konkrétne funkcie a činnosti, ktoré majú byť outsourcované. Rámec opatrení, ktorý je daný výsledkami predchádzajúceho hodnotenia rizika, by mal byť určujúci pre stupeň a hĺbku požadovanej zmluvnej ochrany ešte pred tým, ako sa tieto činnosti vykonajú.
Zmluvy musia odrážať odsúhlasené bezpečnostné opatrenia a schválenia od príslušných vlastníkov procesov ešte predtým, ako dôjde k uzatvoreniu a plneniu zmluvy. Zmluvy musia byť preskúmané príslušnými zainteresovanými stranami spoločnosti GAMO a.s., odsúhlasené a podpísané oboma stranami.
Rámec opatrení by mal určovať dodávateľovi súbor štandardných prvkov a modelov, ktoré MUSIA BYŤ dôsledne začlenené do všetkých zmlúv o outsourcingu. Tie by mali zahŕňať najmä:

a) dodržiavanie osvedčených postupov v oblasti informačnej bezpečnosti,
b) zabezpečenie dôvernosti, integrity a dostupnosti prenášaných a spracúvaných informácií,
c) včasné hlásenie bezpečnostných incidentov,
d) obmedzenie fyzického a logického prístupu k aktívam, priestorom a informáciám,
e) ochrana osobných údajov,
f) dodržiavanie príslušných právnych a regulačných požiadaviek,
g) dodržiavanie protokolov o subdodávkach voči iným poskytovateľom služieb outsourcingu, dodávateľom,
h) bezpečné vrátenie, prenos alebo zničenie hardvéru, softvéru a informácií pri skončení zmluvného vzťahu,
i) kvalita a úroveň služieb,
j) účinné opatrenia na zabezpečenie kontinuity činností,
k) licenčné požiadavky a práva duševného vlastníctva,
l) ošetrenie práva na audit a poskytnutie primeraných záruk (napríklad nezávislý audit, certifikácia, atď.).

MUSÍ existovať formálny zdokumentovaný proces na riešenie akýchkoľvek bezpečnostných problémov alebo incidentov prostredníctvom dohodnutého kontaktného miesta poskytovateľa služieb outsourcingu.

1.6 Cloudové služby

Na podporu obstarania alebo využívania cloudových služieb MUSÍ BYŤ nasadený formálny a zdokumentovaný proces ktorý, bude v súlade s rámcom bezpečnostných opatrení a uplatňovaný v celej organizácii.
Programy zvyšovania povedomia zabezpečujú, že zamestnanci sú si vedomí pozície organizácie v oblasti využívania služieb založených na cloudových službách, rozumejú rizikám spojeným s používaním neschválených cloudových služieb a dôsledne dodržiavajú firemné požiadavky na obstaranie a využívanie externých služieb.

Pred obstaraním alebo použitím cloudových služieb je vykonané posúdenie rizika. Mala by sa pri tom vziať do úvahy povaha a kritickosť / citlivosť informácií, ktoré sú predmetom služby a súvisiace právne a regulačné riziká, a to pre celý životný cyklus informácií.
Rámec opatrení definuje požiadavky týkajúce sa ukladania, šifrovania a spracovania údajov na základe úrovne rizika a klasifikácie informácií, s ohľadom na ich fyzickú lokáciu uloženia (reflektujúc na zákonné a iné regulačné požiadavky platné na území, v rámci ktorého sa údaje nachádzajú), ktoré sa majú spracovávať v príslušnej cloudovej službe.
Rámec opatrení zabezpečí bezpečnosť a dostupnosť citlivých informácií uložených alebo spracovaných v cloude pomocou:

a) ochrany informácií proti ich zámene pomocou primeraných fyzických a logických opatrení,
b) vývoja technickej bezpečnostnej infraštruktúry, ktorá je kompatibilná s architektúrou a infraštruktúrou poskytovateľa cloudových služieb,
c) udržiavania kompatibility a stavu bezpečnosti klientskych systémov používaných na prístup ku cloudovým službám,
d) používania bezpečných komunikačných mechanizmov na prístup k cloudovým službám,
e) zabezpečenia prispôsobiteľných sieťových prepojení, viacerých komunikačných kanálov a primeranej šírky pásma.

Zmluvy o poskytovaní cloudových služieb MUSIA BYŤ uzavreté s ustanoveniami, ktoré sa vzťahujú na štandardné externé dodávateľské zmluvy a zahŕňajú zároveň aj ďalšie špecifické bezpečnostné opatrenia.
Rámec opatrení na ochranu údajov spracovávaných v cloude by mal zahŕňať najmä:

a) poskytovanie zabezpečenej autentifikačnej služby, ktorá spĺňa požiadavky na manažment identít v Organizácii,
b) obmedziť prístup k informáciám len pre oprávnených používateľov,
c) riadenie prístupu ku cloudovým službám pre tie spojenia, ktoré vznikli mimo firewallu Organizácie,
d) zavedenie mechanizmov ochrany proti škodlivému kódu,
e) vykonávanie bezpečného zničenia údajov podľa požiadaviek na ochranu firemných záznamov,
f) vyžadovať, aby poskytovatelia cloudových služieb zdieľali údaje o nezvyčajných alebo škodlivých aktivitách,
g) chrániť osobné údaje a umiestniť ich v rámci schválených lokácií alebo v konkrétnej jurisdikcii, ktorá chráni obchodnú pozíciu a záujmy Organizácie,
h) splnenie požiadaviek na dostupnosť údajov prostredníctvom poskytnutia špecializovanej podpory v prípade bezpečnostného incidentu alebo právneho konania (napríklad žiadostí o súčinnosť zo strany orgánov činných v trestnom konaní) a poskytnutia úschovy údajov prostredníctvom dôveryhodného dodávateľa, ak je to vhodné,
i) poskytovať vopred oznámenie o akýchkoľvek zmenách v službe, ktoré zahŕňajú infraštruktúru, významnú rekonfiguráciu poskytovania cloudových služieb alebo zabezpečenia, spracovanie údajov v novej geografickej alebo právnej jurisdikcii a využívanie subdodávateľov.

1.7 Prenos dát k dodávateľom

Rámec opatrení definuje a presadzuje príslušné a primerané opatrenia na prenosy informácií (fyzických alebo elektronických) na externých subdodávateľov na základe výsledkov posúdenia rizika a bezpečnostných požiadaviek na citlivé informácie.
Zoznam prenosov údajov ku externým dodávateľom je v súlade s formálnym zdokumentovaným procesom udržiavaným naprieč všetkými divíziami GAMO a.s.

Programy zvyšovania povedomia zabezpečujú, že zamestnanci GAMO a.s. sú si vedomí štandardných prevádzkových postupov a kontrol vytvorených na ochranu informácií zasielaných alebo prijatých od externých dodávateľov.
Kontrola prenosu údajov externým dodávateľom vrátane podporných komponentov infraštruktúry sa pravidelne prehodnocuje, aby sa zabezpečil súlad s požiadavkami platných bezpečnostných postupov a smerníc prijatých GAMO a.s.
Pre potrebu kopírovania prevádzkových informácií do testovacieho prostredia sú v organizácii prijaté postupy pre riadenie zálohovania, archivácie a obnovy dát. Po ukončení testovania sa z testovacieho prostredia ihneď prevádzkové informácie vymažú.

1.8 Zmenové konanie

V prípade zmenových konaní v kontexte povinností dodávateľov GAMO a.s. definovala postupy pre zmeny v zmluvách, zmeny pri implementácii, zmeny bezpečnostných politík a pracovných postupov, zmeny v opatreniach pre riešenie bezpečnostných incidentov.

1.9 Zoznam dodávateľov

Pre účel riadenia dodávateľských vzťahov GAMO a.s. vedie dokumentáciu vrátane identifikácie prvkov v správe dodávateľov - vo forme zoznamu aktív, kategorizácie sietí a informačných systémov.

GAMO a.s. vyhlasuje, že bude vždy pri uzatváraní spoluprác s dodávateľmi vykonávať relevantnú analýzu rizík v potrebnom rozsahu s cieľom definovať bezpečnostné postupy, ktoré sa majú prerokovať a dohodnúť vrátane zmluvných vymedzení.

GAMO a.s. vyhlasuje, že do zmlúv s externými dodávateľmi vždy vkladá klauzulu o dodržiavaní bezpečnostných zásad, noriem a postupov zavedených v organizácii.

1.10 Zmluvy s dodávateľmi a tretími stranami

Podmienky pre externých dodávateľov sú definované v zmluvách. S každým dodávateľom je uzatvorená zmluva alebo dohoda o poskytnutí služieb (napríklad Zmluva o poskytovaní služieb, Rámcová zmluva o spolupráci, Zmluva o dielo), ako určujú kapitoly 7, 8, a 9.
GAMO a.s. zabezpečuje evidenciu všetkých uzatvorených zmlúv s dodávateľmi a vyhlasuje, že táto evidencia je súčasťou bezpečnostnej dokumentácie v kontexte požiadavky na zadokumentovanie vymedzenia rozsahu a spôsobu plnenia bezpečnostných opatrení.
Ak je predmetom dodávky pre spoločnosť GAMO a.s. taký typ služieb, ktoré priamo súvisia s prevádzkou sietí a informačných systémov GAMO a.s. ako prevádzkovateľa základnej služby, a poskytovanie služieb priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov GAMO a.s., s uvedeným typom dodávateľa je okrem zmluvy alebo dohody o poskytnutí služieb povinne uzatvorená aj **zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností v súlade s požiadavkou § 19 ods. 2 zákona 69/2018 Z.z.** počas celej doby platnosti zmluvy. Určené podmienky definujú stanovené bezpečnostné pravidlá na zabezpečenie súladu s bezpečnostnou politikou kybernetickej bezpečnosti organizácie. Zmluvy sú vždy podpísané výhradne pred poskytnutím prístupu k aktívam organizácie.
GAMO a.s. vyhlasuje, že každá zmluva uzatvorená s treťou stranou obsahuje minimálne bezpečnostné opatrenia pre oblasť:

- riešenia kybernetických bezpečnostných incidentov,
- riadenia prístupov,
- riadenia bezpečnosti sietí a informačných systémov,

- technických zraniteľností systémov a zariadení,
- monitorovania, testovania bezpečnosti a bezpečnostných auditov.

GAMO a.s. rovnako kladie dôraz na zmluvné strany s tretím stranami, pričom do zmlúv s nimi v súlade s požiadavkami legislatívy v oblasti kybernetickej bezpečnosti pre prevádzkovateľov základnej služby zapracúva:

a) obdobie trvania zmluvy,
b) ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
c) ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou, konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana, a vyjadrenie súhlasu s nimi,
d) konkrétny rozsah činností tretej strany,
e) ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
f) zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 Zákona o KB 69/2018 Z.z.,
g) ustanovenie o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
h) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
i) ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
j) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane,
k) ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
l) záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu,
m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
n) ustanovenie o podmienkach a spôsobe ukončenia zmluvy,
o) záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup, prevádzkovateľovi základnej služby.

Zmluva s treťou stranou obsahuje bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 2 písm. zákona č. 69/2018 Z.z. v znení neskorších predpisov:

f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,

k) bezpečnosť pri prevádzke sietí a informačných systémov,

l) ochranu proti škodlivému kódu a nežiaducemu obsahu,

n) monitorovanie, zaznamenávanie a hlásenie udalostí,

q) dodávateľský reťazec,

Konkrétny rozsah opatrení sa určí na základe vykonanej analýzy rizík ešte pred uzatvorením zmluvného vzťahu s treťou stranou.
Evidencia všetkých uzatvorených zmlúv s tretími stranami je súčasťou bezpečnostnej dokumentácie GAMO a.s.

1.11 Vzdelávanie pracovníkov dodávateľov

GAMO a.s. identifikovala a zdokumentovala koordináciu a dohľad nad aspektmi kybernetickej a informačnej bezpečnosti vo vzťahoch s dodávateľmi. Pracovníci dodávateľa sú povinní oboznámiť sa s požiadavkami v oblasti bezpečnostného povedomia a zavedenej bezpečnostnej dokumentácie.

GAMO a.s. pre tento účel implementovala proces preukázateľného poučenia/oboznámenia/zvyšovania bezpečnostného povedomia pracovníkov dodávateľa, pričom GAMO a.s. pravidelne hodnotí účinnosť plánu rozvoja bezpečnostného povedomia pracovníkov dodávateľa. Kontroly dodržiavania bezpečnostných pravidiel zo strany pracovníkov dodávateľov sú realizované raz ročne hodnotením Plnenia opatrení IB prostredníctvom Hodnotiacich formulárov, ktoré sú prílohami F-02, F-03, F-04 tejto smernice.

1.12 Disciplinárny proces

Porušenie zavedených bezpečnostných pravidiel v oblasti riadenia dodávateľských vzťahov bude riešené sankciami, ktoré sú uvedené v zmluve s dodávateľom. To platí aj pre akékoľvek narušenie bezpečnosti organizácie zo strany osôb dodávateľov zastávajúcich niektorú z bezpečnostných rolí a iných pracovných pozícií.

2. Podmienky na zabezpečenie BOZP a OPP

2.1 Všeobecne

Dodávateľ prác a služieb je povinný dodržiavať „Podmienky a povinnosti na zabezpečenie bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi pre dodávateľov prác a služieb v objektoch a na pracoviskách GAMO a.s., (ďalej len „Podmienky BOZP a OPP a environmentu“) a je povinný zaistiť dodržiavanie týchto podmienok u všetkých jeho pracovníkov“ (vrátane pracovníkov subdodávateľa), ktorí budú pre neho vykonávať dohodnuté práce/služby.

Vybranému dodávateľovi sú spolu s objednávkou resp. zmluvou sprístupnené na web stránke spoločnosti aj Podmienky BOZP a OPP a environmentu, ktoré je dodávateľ povinný počas prác a poskytovania služieb dodržiavať. Podmienky BOZP a OPP sú uvedené v Prílohe F-08-S-00-21 tejto smernice.

2.1.1 Povinnosti dodávateľa oblasť BOZP a OPP

Dodávateľ prác a služieb sa zaväzuje pri realizácii dohodnutých dodávateľských prác a služieb fyzických osôb, ktorí sú podnikateľmi SZČO a právnických osôb, ktorých zamestnanci vykonávajú na jeho pracoviskách montážne, opravárenské, stavebné a iné práce dodržiavať povinnosti definované v prílohe F-09-S-00-21 „Podmienky BOZP a OPP a environmentu“ pre výkon dodávateľských práce.

a) Pred začatím prác/služieb zabezpečiť preukázateľné oboznámenie všetkých pracovníkov, ktorí budú vykonávať dohodnuté práce/služby s Podmienkami BOZP a OPP.
b) Odovzdať „Platné povolenia na prácu v zmysle prílohy F-09-S-00-21.

c) Zabezpečiť opakované oboznámenie všetkých pracovníkov 1x za 3 roky s Podmienkami BOZP a 1x za 2 roky s OPP a na vyžiadanie zo strany poverenej osoby GAMO a.s. predložiť originál z oboznámenia.
d) Práce vykonávať len odborne spôsobilými osobami s príslušným dokladom v zmysle zákona 124/2006 Z. z. v prípade, že to tento zákon vyžaduje.

V prvý deň príchodu dodávateľa na pracovisko je koordinátor za GAMO a.s. (ďalej len KD) zodpovedný za kontrolu oboznámenia všetkých zamestnancov dodávateľa vrátane subdodávateľov s podmienkami BOZP a OPP. Po vykonaní oboznámenia KD preberie od zodpovednej osoby dodávateľa a služieb kópie všetkých požadovaných dokladov o oboznamovaniach a všetky kópie preukazov vyžadovaných k vykonávanej činnosti. V prípade, ak sú všetky vyžadované doklady správne a platné, KD vypíše dodávateľovi povolenie na prácu. Všetky kópie dokladov sú súčasťou dokumentácie k danej práci, ktorú si vedie KD. V prípade, ak sa v prvý deň prác nedostavia na pracovisko spoločnosti GAMO a.s. všetky osoby, ktoré budú práce vykonávať, je potrebné, aby boli prostredníctvom KD oboznámení s podmienkami tejto smernice v prvý deň ich príchodu do spoločnosti GAMO a.s.. KD týmto osobám dodatočne vypíše nové povolenie na prácu.

2.2 Výkon prác

Pred samotným výkonom prác KD spolu so zodpovednou osobou dodávateľa vykonajú hodnotenie rizík k danej práci a spolu nastavia podmienky danej práce. Všetky podmienky vrátane riadenia prípadného rizika sú zaznačené **v povolení na prácu príloha F-09-S-00-21 tejto smernice.** Po vydaní povolenia na prácu prostredníctvom KD je dodávateľovi odovzdané pracovisko na dobu potrebnú pre výkon daných prác, táto doba je uvedená v povolení na prácu.

Ak je výsledkom hodnotenia rizík ohrozenie interných zamestnancov spoločnosti GAMO a.s. a nie je možné technickým alebo iným obdobným spôsobom dané riziko vylúčiť, je KD povinný oboznámiť všetkých interných zamestnancov spoločnosti GAMO a.s. s možným rizikom a so spôsobom jeho riadenia, t. j. opatreniami na jeho minimalizáciu na čo najnižšiu možnú mieru.

V prípade, ak sa počas prác zmenia podmienky BOZP, resp. OPP, je zodpovedná osoba dodávateľa povinná ihneď zastaviť všetky vykonávané práce a oboznámiť s touto skutočnosťou KD. Následne spolu s KD vykonajú opätovné prehodnotenie rizík a následne vydajú nové povolenie na prácu s uvedením nových zistených skutočností. Povolenie na prácu je vždy vydávané dvojmo, originál je povinný uchovávať zodpovedná osoba dodávateľa a kópiu KD.

KD je povinný počas výkonu prác vykonávať kontroly dodržiavania náležitostí povolenia na prácu, v prípade, ak zistí nesúlad medzi podmienkami uvedenými v povolení na prácu a výkonom práce, je povinný všetky práce zastaviť a žiadať od dodávateľa vykonanie nápravy. Túto skutočnosť KD zaznačí do povolenia na prácu.

Povolenie na prácu je vydávané len na čas nevyhnutne potrebný na výkon práce na pracovisku spoločnosti GAMO a.s..

Ak dodávateľ vykonáva v spoločnosti GAMO a.s. pravidelne tú istú prácu s tými istými osobami, je možné vydať dané povolenia na prácu na max. dobu jeden kalendárny rok. Po uplynutí tejto lehoty je KD povinný vydať nové povolenie na prácu na ďalší kalendárny rok. Pri týchto prácach je povinnosťou KD si pred začiatkom každého samostatného výkonu práce skontrolovať všetkých členov pracovnej skupiny a v prípade nových členov postupovať podľa vyššie uvedených pravidiel.

2.3 Výkon práce pri spolupráci dodávateľských organizácií

Pri práci viacerých dodávateľov na jednom pracovisku platia tie isté podmienky, ako sú popísané vyššie, navyše sú určení pre každú samostatnú pracovnú skupinu samostatné zodpovedné osoby dodávateľa. Za práce interných zamestnancov spoločnosti GAMO a.s. úlohu preberá KD. V prípade zistenia akéhokoľvek nedostatku je zodpovedná osoba dodávateľa, ktorá nedostatok spôsobila, resp. našla, povinná oznámiť túto skutočnosť nielen KD, ale aj zodpovedné osoby ostatných dodávateľov.

3. Povinnosti dodávateľa v oblasti ENVIRONMENTU

Spoločnosť GAMO a.s. vyžaduje od dodávateľov riadne plnenie povinností zodpovedného environmentálneho správania sa, ktoré vyplýva z platnej legislatívy v oblasti životného prostredia a to najmä:
Zákon č. 79/2015 Z. z. o odpadoch,
Zákon č. 364/2004 Z. z. o vodách,
Zákon č. 137/2010 Z. z. o ovzduší,

Dodávateľ sa pri plnení zmluvných povinností v priestoroch zaväzuje:

a) Dodávateľ, ktorý je povinnou osobou podľa zákona o odpadoch v znení neskorších predpisov je povinný na vyžiadanie preukázať v lehote 10 dní, že si plní povinnosti podľa § 27 ods. 4 tohto zákona. Pri dodávke tovarov, ktoré sú balené do takých druhov obalov, na ktoré sa vzťahuje zákon č. 79/2015 Z. z. o odpadoch je povinný na požiadanie objednávateľa preukázať splnenie povinností podľa zákona č. 79/2015 Z. z. o odpadoch, najmä predložením platnej zmluvy s organizáciou zodpovednosti výrobcov alebo iného relevantného dokladu potvrdzujúceho zabezpečenie plnenia povinností rozšírenej zodpovednosti výrobcu.

b) Nahradiť akúkoľvek škodu, ktorá by jej vznikla v súvislosti s čo i len čiastočnou nepravdivosťou tohto vyhlásenia alebo neplnením jeho povinnosti podľa platného zákona o odpadoch. Dodávateľ berie na vedomie, že škodou sa rozumie akákoľvek majetková i nemajetková ujma, ktorá spoločnosti vznikne v súvislosti s porušením tohto vyhlásenia alebo porušením akejkoľvek povinnosti vyplývajúcej z platného zákona o odpadoch.

c) Zneškodňovať na miestach realizácie zákazky odpad podľa kategórií odpadu na vlastné náklady a v súlade s požiadavkami menovanej legislatívy.
d) Nakladať s odpadom, ktorý vzniká v dôsledku stavebnej činnosti v priestoroch GAMO v súlade s platnými legislatívnymi ustanoveniami.
e) Pri požiadavke na zber a spracovanie nebezpečných odpadov musí mať dodávateľ uzatvorenú zmluvu o preprave s kvalifikovaným zberateľom odpadov alebo spracovateľskou spoločnosťou.
f) Ak vykonávané práce vyžadujú, aby príslušný subjekt prevzal do vlastníctva alebo zabezpečil likvidáciu nebezpečného odpadu alebo elektronického šrotu, dodávateľ sa musí obrátiť na zástupcu GAMO a.s., aby mu poradil pri výbere dodávateľov na spracovanie.

Ing. Kristián Alakša
Generálny riaditeľ