



Poučenie o zásadách informačnej bezpečnosti pre tretie strany a poučenie oprávnenej osoby

Zhrnutie: Tento dokument definuje základné bezpečnostné požiadavky na tretiu stranu*, ktorá vzhľadom na obchodný vzťah so spoločnosťou Orange Slovensko, a.s. (ďalej iba „Orange“) musia mať prístup do fyzických priestorov spoločnosti Orange a/alebo k počítačovým systémom a sieťam (ďalej informačné systémy) v **prostredí spoločnosti Orange. Cieľom je minimalizovať bezpečnostné riziká spojené s pôsobením tretej strany v prostredí spoločnosti Orange a preniesť na ňu zodpovednosť za možné následky nedodržovania týchto bezpečnostných požiadaviek. Tretia strana sa zaväzuje tieto požiadavky dodržiavať.

* Za tretiu stranu sa pre účely tohto dokumentu považuje Dodávateľ v súlade so Všeobecnými podmienkami nákupu spoločnosti Orange.

** Pod prostredím spoločnosti Orange sa pre účely tohto dokumentu chápu fyzické alebo logické priestory, nad ktorými ma spoločnosť Orange plnú kontrolu, t.j. buď ich priamo vlastní alebo si ich prenajíma.

Obsah:

1.0	Úvod	3
1.1	Aplikovateľnosť	3
2.0	Fyzická bezpečnosť	3
2.1	Základné zásady fyzickej bezpečnosti	3
2.2	Kontrola vstupu	4
2.2.1	Povolenie na vstup	4
2.2.2	Pravidlá vstupu a používanie vstupných kariet	4
2.2.3	Režim prideľovania a používania mechanických kľúčov	5
2.3	Priestory s osobitným režimom	5
3.0	Logická bezpečnosť	5
3.1	Používanie osobných počítačov	5
3.2	Používanie osobných počítačov patriacich spoločnosti Orange	6
3.2.1	Prístup do lokálnej počítačovej siete	6
3.2.2	Prístup na Internet	6
3.2.3	Využívanie E-mailu	7
3.2.4	Autorské práva a softwarové licencie	7
3.2.5	Pravidlá antivírovej ochrany	7
3.3	Používanie osobných počítačov patriacich tretej strane	7
3.3.1	Pravidlá pre používanie softwaru	7
3.3.2	Pravidlá antivírovej ochrany	8
4.0	Ochrana majetku a informácií	8
5.0	Žiadosti, postupy a riadenie výnimiek	8
6.0	Nesúlady s pravidlami	9
7.0	Zodpovednosť za ohlasovanie bezpečnostných incidentov	9
	Dodatok A	10
	Dodatok B	11

1.0 Úvod

Cieľom poučenia je informovať tretiu stranu o bezpečnostných požiadavkách, na základe čoho tretia strana svojim podpisom deklaruje súhlas a vôľu splniť tieto požiadavky.

Tretia strana sa svojim podpisom zaväzuje tieto požiadavky dodržiavať v prehlásení tretej strany. Vzor prehlásenia je uvedený na konci tohto dokumentu (viď Dodatok A).

Tieto zásady platia pre každú tretiu stranu, ktorá má zmluvný vzťah so spoločnosťou Orange, na základe ktorého sa stáva súčasťou vnútorného prostredia spoločnosti počas doby nevyhnutnej na realizáciu dohodnutého diela či projektu.

1.1 Aplikovateľnosť

Uvedená tabuľka definuje zoznam kapitol, ktoré sú predmetom poučenia tretej strany, vzťahujúce sa na osoby tretích strán v závislosti od ich prístupu a náplne práce v spoločnosti Orange.

Typ prístupu do spoločnosti Orange	Povinné kapitoly (vrátane všetkých podkapitol)	Poznámka
Osoby LEN s fyzickým prístupom do prostredia spoločnosti Orange	Kap. 2; 4 až 7	V prípade, že osoba je sprostredkovateľom v zmysle platných právnych predpisov na ochranu osobných údajov byť navyše poučená aj v zmysle Dodatku B.
Osoby s logickým prístupom do prostredia spoločnosti Orange	Kap. 3 až 7	V prípade, že osoba je sprostredkovateľom v zmysle platných právnych predpisov na ochranu osobných údajov byť navyše poučená aj v zmysle Dodatku B.
Osoby s fyzickým aj logickým prístupom do prostredia spoločnosti Orange	Všetky kapitoly tejto procedúry	V prípade, že osoba je sprostredkovateľom v zmysle platných právnych predpisov na ochranu osobných údajov byť navyše poučená aj v zmysle Dodatku B.

2.0 Fyzická bezpečnosť

2.1 Základné zásady fyzickej bezpečnosti

Pod fyzickými priestormi, ktorých sa týkajú pravidlá uvedené v tomto dokumente, sa myslia administratívne a technologické priestory vrátane príslušenstva (kuchynky, chodby, toalety, sprchy, sklady a pod.), ktoré spoločnosť Orange dočasne alebo trvale užíva pre výkon svojich podnikateľských činností. Zároveň ide o priestory, v rámci ktorých spoločnosť Orange vykonáva elektronickú alebo fyzickú kontrolu vstupu, príp. pohybu v týchto priestoroch. Táto definícia sa netýka priestorov trvale prístupných verejnosti bez akejkoľvek kontroly vstupu.

Všeobecne platí pravidlo, že vstup každej osoby do priestorov spoločnosti Orange je kontrolovaný. Akákoľvek osoba tretej strany môže vstupovať iba do tých priestorov, do ktorých získala povolenie na vstup.

Vstup a pohyb oprávnených osôb tretích strán sa musí obmedziť iba na čas nevyhnutne potrebný na výkon činností tejto osoby, ktorými bola poverená.

Do priestorov spoločnosti Orange je povolené vnášanie iba takých vecí, okrem bežných osobných vecí, ktoré sú nevyhnutné na výkon činnosti tretej strany. Osobitne je zakázané vnášať do priestorov spoločnosti Orange osobné počítače, zariadenia na ukladanie elektronických informácií a nosiče elektronických informácií (napr. notebooky, USB disky, prenosné pevné disky, prenosné napaľovačky a pod.), pokiaľ tieto zariadenia neslúžia výlučne na výkon činností tretej strany v priestoroch spoločnosti



Orange.

Je prísne zakázané z priestorov spoločnosti Orange vynášať akékoľvek technické zariadenia, počítače, nosiče informácií, dokumenty a iné veci patriace spoločnosti Orange, pokiaľ to nie je nevyhnutné na výkon činností tretej strany v súlade s príslušnou zmluvou.

Tento dokument neupravuje bezpečnosť a ochranu zdravia pri práci a protipožiarnu ochranu v rámci priestorov spoločnosti Orange.

2.2 Kontrola vstupu

Do priestorov spoločnosti Orange môže vstupovať iba oprávnená osoba tretej strany:

- ktorá je vybavená prístupovou kartou a identifikačnou kartou spoločnosti Orange vydanou na jej meno, alebo,
- ktorá je sprevádzaná zamestnancom spoločnosti Orange.

Základná kontrola vstupu je vykonávaná prostredníctvom systému elektronickej kontroly vstupu (VS) a to na základe pridelovania a používania bezkontaktných prístupových kariet. Iba výnimočne a to pre priestory, v ktorých nie je inštalovaný elektronický systém kontroly vstupu, sa kontrola vykonáva riadením pridelovania a používania mechanických kľúčov.

2.2.1 Povolenie na vstup

Všeobecne platí zásada, že vstup každej osoby zastupujúcej tretiu stranu musí byť povolený. Pre oprávnené osoby tretej strany sa povoľuje vstup iba do tých priestorov, ktoré nevyhnutne súvisia s výkonom činností príslušnej osoby. Podmienkou na povolenie vstupu do priestorov spoločnosti Orange (okrem režimu návštev) je minimálne:

- existencia právneho vzťahu medzi treťou stranou a spoločnosťou Orange,
- prehlásenie žiadajúcej osoby tretej strany, že bola poučená o pravidlách uvedených v tomto dokumente alebo v Bezpečnostnej politike spoločnosti Orange pre tretie strany a že sa zaväzuje ich dodržiavať,
- prehlásenie o poučení týkajúcom sa ochrany osobných údajov, ktoré sa môžu nachádzať v priestoroch alebo v informačných systémoch spoločnosti Orange (viď. Dodatok B).

Povolenie na vstup vo forme pridelenia vstupnej karty sa udeľuje na meno konkrétnej osoby. Povolenie na vstup pre oprávnenú osobu tretej strany vybavuje zamestnanec spoločnosti Orange, ktorý zodpovedá za činnosť tretej strany, predpísaným spôsobom na oddelení Orange CorpSec.

2.2.2 Pravidlá vstupu a používanie vstupných kariet

Vstupná karta je neprenosná a oprávňuje na vstup iba tú osobu, na ktorej meno bola vydaná. Používanie prístupovej karty alebo identifikačnej karty inou osobou alebo jej požičiavanie (odovzdanie, sprístupnenie) inej osobe je prísne zakázané.

Držiteľ vstupnej karty je oprávnený používať ju iba na vstup do priestorov, do ktorých má vstup povolený. Ak je priestor, do ktorého oprávnená osoba vstupuje zabezpečený čítacím zariadením VS, je použitie vstupnej karty vždy povinné a to aj v prípade, ak dvere do priestoru sú otvorené (napr. inou vchádzajúcou osobou). Rovnako je potrebné použiť vstupnú kartu vždy pri hlavnom vstupe do priestorov spoločnosti Orange (napr. turnikety na hlavnom vstupe), a to aj v prípade, ak osoba vstupuje napr. pri vnášaní materiálu osobitným nekontrolovaným vstupom (nákladné dvere, brány, rampy a pod.). Pri vstupe do priestorov mimo bežných pracovných hodín môže byť bezpečnostnou službou vyžadovaná osobitná registrácia do knihy návštev a to aj v prípade, ak osoba má povolený vstup do priestorov spoločnosti Orange na základe pridelenej vstupnej karty.

Držiteľ vstupnej karty je ďalej povinný vstupnú kartu chrániť pred jej poškodením, zničením alebo stratou.

V prípade odcudzenia alebo straty vstupnej karty je jej držiteľ povinný bezodkladne oznámiť túto skutočnosť príslušnému zodpovednému pracovníkovi spoločnosti Orange, ktorý zodpovedá za činnosť tretej strany, pracovníkom Úseku ľudských zdrojov (HR) alebo spoločnosti Orange CorpSec (t. č. 0908 004 112, e-mail: xsm_admin@orange.sk).

Oprávnené osoby tretej strany majúce svoje trvalé pracovisko v priestoroch spoločnosti Orange musia okrem vstupných kariet používať identifikačné karty spoločnosti Orange s farebnou fotografiou, logom spoločnosti Orange, menom a názvom pozície a firmy, ktorú zastupujú.

ZA POUŽÍVANIE VSTUPNEJ KARTY, ALE AJ ZA JEJ PRÍPADNÉ ZNEUŽITIE, JE VŽDY ZODPOVEDNÁ OSOBA, KTOREJ BOLA KARTA PRIDELENÁ !!!

2.2.3 Režim pridelenia a používania mechanických kľúčov

Mechanické kľúče je možné prideliť iba v prípade, ak vstup do priestorov, v ktorých oprávnená osoba tretej strany má vykonávať činnosť podľa príslušnej zmluvy, nie je možný iba za použitia vstupnej karty, alebo ak ide o priestory, ktoré nie sú kontrolované elektronickým SV.

Ak ide o priestor, ktorý je kontrolovaný SV a zároveň je potrebné použitie mechanického kľúča, je oprávnená osoba povinná použiť mechanický kľúč a vstupnú kartu vždy súčasne, t.j. nie je povolené použiť iba kľúč bez priloženia vstupnej karty k čítaciemu zariadeniu SV.

POUŽÍVANIE TZV. UNIVERZÁLNEHO KLÚČA SA ZAKAZUJE !!!

Povoľovanie vstupu do priestorov, ktoré sú prístupné prostredníctvom použitia mechanického kľúča, pridelenie kľúčov a ich použitie sa riadi osobitnými pravidlami stanovenými Oddelením Facility na Úseku ľudských zdrojov, príp. pravidlami stanovenými v príslušnej zmluve s treťou stranou.

Ak také pravidlá neboli vydané, alebo sa tretia strana nezaviazala takýmto pravidlám dodržiavať, riadi sa pridelenie a používanie mechanických kľúčov ustanoveniami bodu 2.2 tohto dokumentu, s výnimkou, že poškodenie, zničenie alebo strata mechanického kľúča sa bezodkladne nahlasuje príslušnému zodpovednému pracovníkovi spoločnosti Orange, ktorý zodpovedá za činnosť tretej strany, alebo pracovníkom Úseku ľudských zdrojov (HR).

2.3 Priestory s osobitným režimom

Vstup do priestorov, ktoré majú byť podľa interných bezpečnostných procedúr osobitne chránené (kancelárie vrcholového manažmentu, priestory spoločnosti Orange CorpSec, s.r.o., sklady tovaru a materiálu, pokladne, vybrané zasadačky, technologické miestnosti a pod.), je viazaný na povolenie riaditeľa príslušného úseku spoločnosti Orange. Oprávnené osoby tretích strán môžu vstupovať a pohybovať sa v týchto priestoroch iba za prítomnosti povereného zamestnanca spoločnosti Orange, ak v zmluve s treťou stranou alebo v príslušnom povolení na vstup nie je určené inak.

Ak je tretím stranám povolený vstup do priestorov spoločnosti Orange, ktoré sú monitorované poplachovým systémom narušenia (PSN), môžu do týchto priestorov vstupovať iba, ak im bol pridelený unikátny prístupový kód k PSN.

3.0 Logická bezpečnosť

Pod logickým prostredím, na ktoré sa vzťahujú pravidlá uvedené v tomto dokumente, sa myslia informačné systémy v prostredí spoločnosti Orange, ktoré spoločnosť Orange dočasne alebo trvale užíva pre výkon svojich podnikateľských činností.

Pre logické prostredie všeobecne platí, že prístupy tretích strán do informačných systémov spoločnosti Orange sú riadené a realizované výhradne cez Identity Access Management (ďalej len IAM). Iný spôsob pridelenia prístupu nie je možný. Prístupy do informačných systémov pre zamestnancov tretích strán riadia výhradne interní zamestnanci, ktorí sú zodpovední za tretiu stranu. Akákoľvek osoba tretej strany môže pristupovať iba do tých informačných systémov, do ktorých získala oprávnenie cez IAM.

3.1 Používanie osobných počítačov

Počítač a počítačové zdroje je možné používať len na vopred určený služobný alebo komerčný účel. V prípade pochybností o účele sa použije referencia na konkrétnu zmluvu alebo dohodu o účele prítomnosti tretej strany v spoločnosti Orange. Používanie takýchto zariadení na súkromné účely je zakázané.

3.2 Používanie osobných počítačov patriacich spoločnosti Orange

Ak bolo zamestnancovi tretej strany umožnené používať osobný počítač alebo počítačové zariadenie patriace spoločnosti Orange, nesmie najmä:

- premiestňovať ho (pokiaľ sa nejedná o prenosné zariadenie ako je napr. tablet, notebook a je to nevyhnutné pre plnenie zmluvy),
- ho otvárať, rozoberať,
- pripájať alebo odpájať jeho periférne zariadenia,
- inštalovať naň žiadny software vrátane ovládačov pre hardware či software apod.,
- ak je počítač zapojený do lokálnej počítačovej siete spoločnosti Orange nesmie z neho vytvárať ďalšie, nekontrolované spojenia na iné počítače a systémy (hlavne na Internet), napr. cez wireless LAN (Wi-Fi), GPRS apod. Túto problematiku rieši v spoločnosti Orange výhradne autorizovaný IT personál (HelpDesk).

Ďalšie pravidlá pre tretie strany ako aj ich zamestnancov, súvisiace s používaním osobných počítačov patriacich spoločnosti Orange, sú definované v nasledujúcich kapitolách.

3.2.1 Prístup do lokálnej počítačovej siete

Ak dostane tretia strana v spoločnosti Orange prístup k lokálnej počítačovej sieti:

- musí mať svoje sieťové (Windows doménové) účty pomenované podľa priezviska používateľa a príznaku označujúceho tretiu stranu (externistu, viď časť o používaní e-mailu nižšie); takýto účet nesmie nikdy dostať privilégia lokálneho administrátora inak ako riadeným procesom,
- nesmie poskytnúť svoje autentifikačné údaje k účtu inej osobe – používateľ účtu je v každom prípade zodpovedný za používanie jemu prideleného účtu,
- musí chrániť prístup k svojmu počítaču, ak sa práve nepoužíva,
- nesmie používať lokálne zdieľané adresáre (Windows shares) na výmenu dát medzi ďalšími používateľmi (na tento účel je obvyčajne určený file server manažovaný dôveryhodnou stranou, napr. HelpDesk alebo administrátor domény).

3.2.2 Prístup na Internet

Ak bolo zamestnancovi tretej strany povolené využívať prístup na Internet z lokálnej siete spoločnosti Orange, nesmie:

- prístupovať na stránky s anarchistickým, teroristickým alebo pornografickým obsahom vrátane stránok obsahujúcich ilegálny software a hackerských stránok,
- sťahovať nadmerné objemy dát pokiaľ nemajú súvis s potrebami spoločnosti Orange alebo s účelom pobytu tretej strany v spoločnosti Orange,
- sťahovať software pre osobné, non-business použitie,
- používať Internet na súkromné, či iné komerčné účely,
- používať internetové spojenie na sociálne siete, chatové skupiny/služby, na používanie web-mailových služieb, na odosielanie a sťahovanie súborov z verejných, alebo súkromných web-sharing serverov, alebo na výmenu súborov prostredníctvom p2p sietí a podobne, najmä ak nesúvisia s účelom pobytu tretej strany v spoločnosti Orange,
- pokúšať sa získať neautorizovaný prístup do vzdialených počítačových systémov alebo k súborom v internete, alebo intranete,
- porušovať súkromie iných používateľov Internetu (spam, sociálny inžiniering apod.),
- prístupovať na Internet priamo z takzvaných "produkčných" systémov,
- vytvárať HTTP tunely (napr. enkapsuláciou iných protokolov v rámci HTTP) do verejných (Internet) zdrojov.

3.2.3 Využívanie E-mailu

Ak bolo zamestnancovi tretej strany povolené využívať e-mail z lokálnej siete spoločnosti Orange, nesmie:

- vystupovať ani sa podpisovať ako zamestnanec spoločnosti Orange a musí mať v e-mailovej adrese (SMTP) vrátane zobrazovaného mena a aliasov označenie pre externistu (ext, x_, napr. ext_meno.priezvisko@orange.sk)

a tiež nesmie e-mail používať na:

- žiadne účely, ktoré by mohli predstavovať porušovanie platných zákonov Slovenskej republiky,
- súkromné alebo iné komerčné aktivity, ktoré nemajú žiadny vzťah k obchodným záujmom spoločnosti Orange,
- zasielanie spamu s prílohami (obrázky, prezentácie, spustiteľné súbory, iné). Posielanie emailu podlieha interným pravidlám a obmedzeniam spoločnosti Orange,
- šírenie súkromných názorov, "chain letters" alebo nevhodných správ na distribučné zoznamy adresátov alebo na jednotlivcov (ako napr. žiadosti o vyjadrenie politických názorov, žiadosti o dary atď),
- iné konanie, ktoré je v rozpore s dobrými mravmi a môže mať priamy, alebo nepriamy dosah na dobré meno, alebo obchodné aktivity spoločnosti Orange.

3.2.4 Autorské práva a softwarové licencie

S výnimkou servisných a iných zmluvných vzťahov, ktoré to vopred definujú, nesmú zamestnanci tretej strany inštalovať na osobných počítačoch spoločnosti Orange žiadny neautorizovaný software. Na každý software, ktorý sa má používať, musí existovať príslušná licencia, čo je zodpovednosť Orange Slovensko HelpDesk.

3.2.5 Pravidlá antivírovej ochrany

Osobné počítače musia mať vždy nainštalovaný antivírusový software s aktuálnymi definičnými súborami. To je štandardná zodpovednosť HelpDesk. Používateľ počítača nesmie žiadnym spôsobom obmedziť funkčnosť antivírusového softwaru a ak sám zistí, že jeho počítač je bez antivírusovej ochrany alebo bez najnovšieho antivírusového definičného súboru, je povinný o takomto stave okamžite informovať HelpDesk.

3.3 Používanie osobných počítačov patriacich tretej strane

Počítače nepatriace spoločnosti Orange nesmú byť pripájané do lokálnej počítačovej siete spoločnosti Orange a nesmú mať prístup na Internet, len za predpokladu, že tretej strane bola udelená výnimka (viď kapitolu 5.).

Zamestnanci tretích strán nesmú inštalovať alebo používať v spoločnosti Orange svoje vlastné komunikačné zariadenia a používať ich na nekontrolovaný prístup k internetu a zdieľanie informácií. (napr. modemy, faxy, či wi-fi zariadenia.)

Ak bolo tretej strane dovolené používať svoje vlastné počítače v lokálnej počítačovej sieti spoločnosti Orange, musí spĺňať požiadavky uvedené v kapitole 3.2, s výnimkou častí o používaní softwaru (kap. 3.2.4) a o vírusoch (3.2.5), na ktoré sa vzťahujú osobitné ustanovenia definované v nasledujúcich kapitolách.

3.3.1 Pravidlá pre používanie softwaru

Ak sú osobné počítače tretej strany súčasťou lokálnej počítačovej siete spoločnosti Orange, nesmie na nich tretia strana používať software alebo hardware, ktorý je možné zneužiť proti spoločnosti Orange. Patria sem sieťové snifery, analyzátory sieťovej premávky, vírusové toolkity, port scannery, scannery zdieľaných sieťových zdrojov apod.

Zároveň sa predpokladá, že každý software inštalovaný na týchto počítačoch je riadne licencovaný, za čo tretia strana zodpovedá bez ohľadu na licenčné pravidlá a zmluvné záväzky spoločnosti Orange.

3.3.2 Pravidlá antivírovej ochrany

Ak má tretia strana povolené používať v spoločnosti Orange svoje vlastné počítače, je povinná na nich používať riadne aktualizovaný antivírusový software a zodpovedá za prípadne následky pre spoločnosť Orange v prípade vírusového problému, ktorý vznikol pôsobením tretej strany v spoločnosti Orange.

4.0 Ochrana majetku a informácií

Tretím stranám je v priestoroch spoločnosti Orange zakázané:

- akékoľvek vynášanie a premiestňovanie vecí patriacich spoločnosti Orange, alebo jej zamestnancom, osobitne počítačov, počítačových zariadení, iných technológií a pod.,
- zapínanie, vypínanie, alebo akákoľvek iná manipulácia s technickými zariadeniami umiestnenými v priestoroch spoločnosti Orange,

ak tieto činnosti nie sú súčasťou plnení tretej strany na základe príslušnej zmluvy so spoločnosťou Orange.

Ďalej je zakázané:

- vnášať do priestorov spoločnosti Orange osobné počítače, zariadenia na ukladanie elektronických informácií a nosiče elektronických informácií (napr. notebooky, USB disky, prenosné pevné disky, prenosné napalovačky a pod.), pokiaľ tieto zariadenia neslúžia výlučne na výkon činností tretej strany v priestoroch spoločnosti Orange.
- z priestorov spoločnosti Orange vynášať akékoľvek nosiče elektronických informácií, počítače a dokumenty patriace spoločnosti Orange a akokoľvek inak s týmito vecami manipulovať, pokiaľ to výslovne nie je súčasťou plnenia tretej strany v súlade s príslušnou zmluvou.

Zamestnanci tretej strany, ktorí pri poskytovaní svojich služieb prídu do styku s služobnými/obchodnými informáciami alebo osobnými údajmi patriacimi spoločnosti Orange, nesmú tieto informácie použiť, zneužiť, zverejniť ani neoprávnene poskytnúť žiadnym ďalším stranám.

Vzhľadom k tomu, že spoločnosť Orange v súvislosti s vykonávaním svojich podnikateľských činností spracúva vo svojich informačných systémoch osobné údaje, je každá oprávnená osoba tretej strany, ktorej má byť povolený vstup do priestorov a/alebo prostredia spoločnosti Orange, povinná podpísať poučenie o svojich povinnostiach pre prípad, že by prišla do styku s osobnými údajmi, v rozsahu uvedenom v Dodatku B k tomuto dokumentu.

Tretie strany berú na vedomie, že niektoré priestory spoločnosti Orange sú pre účely ochrany majetku monitorované systémom priemyselnej televízie (CCTV) alebo poplachovým systémom narušenia (PSN).

5.0 Žiadosti, postupy a riadenie výnimiek

Všetky žiadosti pre oprávnené osoby tretej strany o prístupy, o pridelenie zdrojov, o pridelenie oprávnení a pod., ktoré sú nevyhnutné na výkon činností tretej strany v spoločnosti Orange sa podávajú prostredníctvom príslušných formulárov (QAF-ov), alebo k tomuto účelu slúžiacich aplikácií (napr. IAM) a za dodržania príslušných interných postupov platných v spoločnosti Orange pre tretie strany.

Ak také žiadosti a postupy nie sú v spoločnosti Orange formalizované a súvisia s pravidlami uvedenými v tejto politike alebo ak ide o akékoľvek výnimky z požiadaviek uvedených v tomto dokumente sa riešia individuálne prostredníctvom Manažéra pre bezpečnosť spoločnosti Orange.

K získaniu súhlasu k neformalizovanej žiadosti alebo k udeleniu výnimky je zvyčajne potrebné doložiť podrobné zdôvodnenie. Žiadosť o udelenie výnimky sa podáva prostredníctvom príslušného manažéra spoločnosti Orange, ktorý koordinuje činnosť tretej strany v spoločnosti Orange.

Relevantný výňatok z písomnej zmluvy medzi spoločnosťou Orange a treťou stranou sa považuje za najvhodnejší argument pre získanie výnimky z týchto bezpečnostných pravidiel pre tretie strany.

6.0 Nesúlady s pravidlami

Nesúlady s požiadavkami uvedenými v tomto dokumente je považovaný za bezpečnostný incident, ktorý sa eskaluje príslušnej manažérskej úrovni, tak v spoločnosti Orange, ako aj u tretej strany, čo v konečnom dôsledku môže viesť k zmluvným sankciám alebo žiadosti o náhradu škody voči tretej strane, alebo k ukončeniu zmluvného vzťahu s treťou stranou na základe príslušných ustanovení zmluvy.

7.0 Zodpovednosť za ohlasovanie bezpečnostných incidentov

Pracovníci tretej strany sú zodpovední za ohlasovanie bezpečnostných incidentov, o ktorých sa pri výkone svojich činností v spoločnosti Orange dozvedia, alebo ktorých sú bezprostrednými svedkami. Za bezpečnostný incident sa považuje taká udalosť, ktorá má znaky kriminálnej aktivity a/alebo ide také porušenie bezpečnostných pravidiel spoločnosti Orange (minimálne definovaných týmto dokumentom), ktoré môže mať dopad na obchodné a podnikateľské záujmy spoločnosti Orange, na jej zákonné povinnosti, či spôsobiť jej negatívnu publicitu.

Medzi udalosťami, ktoré sa automaticky považujú za bezpečnostný incident patria okrem iného:

- voľne dostupné (nezabezpečené) osobné údaje alebo údaje tvoriace telekomunikačné tajomstvo zákazníkov a osobné údaje zamestnancov spoločnosti Orange, či už v papierovej alebo elektronickej podobe
- zverejnenie obchodného tajomstva alebo klasifikovaných informácií spoločnosti Orange
- vydávanie sa za inú osobu s cieľom získať fyzický/logický prístup alebo oprávnenie prístupu do priestorov spoločnosti Orange, alebo k jej zdrojom
- neautorizovaný prístup do fyzických a logických priestorov spoločnosti Orange
- krádež fyzického majetku alebo duševného vlastníctva spoločnosti Orange
- poskytovanie úplatkov za protislužbu
- vyhrážanie sa osobe ujmou na zdraví, na živote alebo na jej majetku

Bezpečnostný incident musí byť včas a s patričnou presnosťou ohlásený príslušnej úrovni riadenia spoločnosti Orange a spoločnosti Orange CorpSec, s.r.o.



Dodatok A

VZOR

Prehlásenia o poučení oprávnenej osoby (pracovníka) tretej strany o pravidlách bezpečnosti v spoločnosti Orange

Dolu podpísaný zamestnanec/spolupracovník tretej strany:

Meno a priezvisko:
Funkcia:
Názov tretej strany:
IČO:

Týmto prehlasujem, že som bol poučený o bezpečnostných pravidlách a zásadách spoločnosti Orange Slovensko, a.s. uvedených v dokumente: Pravidlá fyzickej bezpečnosti pre vstup tretích strán do priestorov spoločnosti Orange Slovensko, a.s., ktorý je súčasťou Zmluvy o, uzatvorenej medzi spoločnosťou Orange Slovensko, a.s. a treťou stranou dňa

Ďalej prehlasujem, že som uvedeným bezpečnostným pravidlám a zásadám rozumel a zaväzujem sa ich pri výkone svojich činností v/ pre spoločnosť Orange Slovensko, a.s. dodržiavať v celom rozsahu.

V Bratislave, dňa.....

.....
Meno a priezvisko
Funkcia



Dodatok B

VZOR

Poučenie osoby, ktorá môže mať prístup k osobným údajom

spracúvaným v informačných systémoch spoločnosti Orange Slovensko, a.s.

(Pozn.: toto poučenie sa týka dodávateľov, ich zamestnancov, príp. iných osôb, ktoré sú oprávnené na vstup do prevádzok, priestorov spoločnosti Orange Slovensko, a.s., alebo ktoré vykonávajú údržbu, opravy, podporu príp. iné činnosti na informačných systémoch spoločnosti Orange Slovensko, a.s.)

Meno:

Pozícia:

(ďalej len „poučená osoba“)

zamestnanec spoločnosti/dodávateľa:

Obchodné meno:

Sídlo/ miesto podnikania:

IČO:, IČ DPH:

Zmluva/Objednávka:, zo dňa:

(ďalej len „partner“)

Týmto potvrdzujem, že som bol, ako osoba oprávnená na vstup do prevádzok a priestorov spoločnosti Orange Slovensko, a.s., alebo vykonávajúca údržbu, opravy, podporu príp. iné činnosti na informačných systémoch spoločnosti Orange Slovensko, a.s.), poučený o nasledovných právach a povinnostiach vyplývajúcich z platných právnych predpisov upravujúcich ochranu osobných údajov, napr. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES; platný slovenský zákon o ochrane osobných údajov; vykonávacie predpisy k uvedeným právnym predpisom a pod. (ďalej len „**platné právne predpisy na ochranu osobných údajov**“) a o zodpovednosti za ich porušenie:

1. Poučená osoba nie je oprávnená spracúvať, odoberať, kopírovať, oboznamovať sa, ani inak nakladať s osobnými údajmi účastníkov verejných komunikačných služieb spoločnosti Orange Slovensko, a.s., alebo s osobnými údajmi zamestnancov spoločnosti Orange Slovensko, a.s. alebo iných dotknutých osôb zhromaždenými v informačných systémoch, príp. v priestoroch spoločnosti Orange Slovensko, a.s.
2. V prípade, ak poučená osoba po vstupe do prevádzok a priestorov spoločnosti Orange Slovensko, a.s. alebo pri výkone údržby, opravy, podpory príp. iných činností na informačných systémoch spoločnosti Orange Slovensko, a.s. príde do styku s osobnými údajmi, je povinná bez zbytočného odkladu akoukoľvek formou informovať o tom zodpovedného zamestnanca spoločnosti Orange Slovensko, a.s..
3. V prípade, ak poučená osoba po vstupe do prevádzok a priestorov spoločnosti Orange Slovensko, a.s., alebo pri výkone údržby, opravy, podpory príp. iných činností na informačných systémoch spoločnosti Orange Slovensko, a.s. získa osobné údaje, je povinná okamžite osobné údaje, resp. nosič, na ktorom sú uložené, alebo zapísané (vrátane papiera), odovzdať zodpovednému zamestnancovi spoločnosti Orange Slovensko, a.s.. Takíto nosič si poučená osoba nesmie v žiadnom prípade kopírovať ani vyhotoviť z neho akúkoľvek rozmnoženinu.



4. Poučená osoba smie vstupovať do informačných systémov spoločnosti Orange Slovensko, a.s. iba v nevyhnutnom rozsahu a iba ak to súvisí s oprávneným výkonom jej činnosti a to po predchádzajúcom upozornení zodpovedného zamestnanca spoločnosti Orange Slovensko, a.s..
5. Poučená osoba nesmie vykonať akýkoľvek zásah do informačného systému spoločnosti Orange Slovensko, a.s., ktorý môže mať za následok jeho zhoršenie, poškodenie, zlyhanie, zničenie, alebo akékoľvek znefunkčnenie. Ak má poučená osoba v súlade s jej oprávneniami na výkon činností na informačných systémoch spoločnosti Orange Slovensko, a.s. vykonať určitý zásah, pri ktorom môže, s prihliadnutím na primeranú odbornú starostlivosť, predpokladať, že takýto zásah môže mať vyššie opísaný vplyv na informačný systém spoločnosti Orange Slovensko, a.s., je povinná vopred o tom upovedomiť zodpovedného zamestnanca spoločnosti Orange Slovensko, a.s..
6. Poučená osoba je povinná zachovávať mlčanlivosť o všetkých osobných údajoch, s ktorými prišla do styku pri vykonávaní svojej činnosti, ako aj o spôsobe a rozsahu ich spracovávaní v informačných systémoch spoločnosti Orange Slovensko, a.s. Poučená osoba je najmä povinná nevyužívať osobné údaje, s ktorými príde do styku pre osobnú potrebu a nesmie ich sprístupniť a poskytnúť tretej osobe, alebo ich zverejniť. Poučená osoba je povinná zachovávať mlčanlivosť podľa tohto bodu aj po ukončení činnosti v spoločnosti Orange Slovensko, a.s.
7. Poučená osoba je povinná pri výkone svojich činností riadiť sa výlučne príslušnými platnými právnymi predpismi na ochranu osobných údajov, zmluvou uzatvorenou medzi ňou resp. jej zamestnávateľom/zmluvným partnerom a spoločnosťou Orange Slovensko, a.s., týmto Poučením a pokynmi spoločnosti Orange Slovensko, a.s., v opačnom prípade poučená osoba v plnom rozsahu zodpovedá za porušenie týchto povinností.

Zároveň ako poučená osoba vyhlasujem, že svojim právam a povinnostiam, o ktorých som bol poučený, rozumiem a zaväzujem sa ich dodržiavať.

V, dňa

.....
Čitateľné meno a podpis poučenej osoby

Za partnera poučenie vykonal:

Meno:, úsek:

Tel.:, fax:, e-mail:

.....
Podpis