**Technicko-organizační předpis pro zajištění ochrany údajů a důvěrnosti komunikací**

**OBSAH:**

**1 ÚVODNÍ USTANOVENÍ .................................................................................................................................................. 3**

1.1 ÚČEL.................................................................................................................................... 3

1.2 PŮSOBNOST ................................................................................................................................................... 3

1.3 ZKRATKY A POJMY ...................................................................................................................................................3

1.4 STRUKTURA DOKUMENTU ............................................................................................................................................…….3

**2 ODPOVĚDNOSTI A PRAVOMOCI ................................................................................................................................................. 4**

2.1 POVINNOSTI ZAJISTIT BEZPEČNOST CHRÁNĚNÝCH ÚDAJŮ VYPLÝVAJÍCÍ PRO SPOLEČNOST ZE ZEKU
(§ 88 ODST. 1, 2, 4 A 5, § 88A ODST. 1 A 2):

................................................................................................................................................... 4

2.2 POSKYTOVÁNÍ SLUŽEB ZA KRIZOVÝCH STAVŮ DLE §99………………………………. 4

**3 NAPLNĚNÍ POŽADAVKŮ ZÁKONA ....................................................................................................................................................5**

3.1 ANALÝZA BEZPEČNOSTNÍCH RIZIK ................................................................................................................................................... 5

3.2 DOPADY NARUŠENÍ BEZPEČNOSTI .................................................................................................................................................. 6

3.3 POKRYTÍ IDENTIFIKOVANÝCH RIZIK .................................................................................................................................................. 6

3.4 ZPRACOVÁNÍ CHRÁNĚNÝCH ÚDAJŮ .................................................................................................................................................. 6

3.5 PŘÍSTUP TŘETÍCH STRAN K CHRÁNĚNÝM ÚDAJŮM .................................................................................................................................................. 6

**4 SOUVISEJÍCÍ DOKUMENTACE .................................................................................................................................................. 7**

4.1 ŘÍDICÍ DOKUMENTY ....................................................................................................................................................7

4.2 ZÁZNAMY ................................................................................................................................................... 7

**5 ZÁVĚREČNÁ A PŘECHODNÁ USTANOVENÍ .................................................................................................................................................. 7**

**1.1 Účel**

Technicko-organizační předpis (dále jen „TOP“) je zpracován na základě povinností vyplývajících pro společnost XXX z ustanovení § 88 a § 88a zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

Cílem tohoto TOP je demonstrovat přístup společnosti k zajištění bezpečnosti poskytovaných služeb s ohledem na ochranu osobních, identifikačních, provozních údajů a důvěrnost komunikací fyzických a právnických osob.

TOP k provedení ustanovení § 88 a § 88a zákona o elektronických komunikacích je v rámci společnosti zpracováván jako součást interních řídicích předpisů.

**1.2 Působnost**

TOP je v celém rozsahu závazný pro všechny zaměstnance XXX, osoby činné pro společnost na základě dohod o pracích konaných mimo pracovní poměr a pro všechny další subjekty, které mají přístup do informačních systémů (dále jen IS) XXX.

**1.3 Zkratky a pojmy**

 **Údaje** –ve smyslu tohoto TOP jsou pod pojem „údaje“ zahrnuty osobní údaje, identifikační údaje a provozní údaje

 **Osobní údaje** – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

 **Identifikační údaje** – údaje týkající se právnické osoby, specifikované v zákonu

 **Provozní údaje** – jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování

 **TOP** – Technicko-organizační předpis

 **ČTÚ** – Český telekomunikační úřad

 **ISMS** – Integrovaný systém řízení bezpečnosti informací

 **IS – informační** systémy společnosti

 **NDA** – Non Disclosure Agreement **–** smlouva o ochraně informací

 **Třetí strany – osoba**, organizace nebo jiná seskupení, která jsou nezávislá na přímo zainteresovaných stranách

 **Chráněné údaje (Informace) -** jakákoli informace, která je považována za neveřejnou

 ZEK – zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

**1.4 Struktura dokumentu**

Dokument je koncipován jako rozhraní mezi zákonnými požadavky a interní řídící dokumentací společnosti. V jednotlivých kapitolách se dokument odvolává na existující dokumentaci (rozhodnutí, směrnice, instrukce), ve které je daný požadavek / problematika řešena.

**2 ODPOVĚDNOSTI A PRAVOMOCI**

Základní odpovědnosti a pravomoci jsou stanoveny v kapitole xx Bezpečnostního řádu a další řídicí dokumentací vztahující se k řízení bezpečnosti.

Za jednotlivé útvary a společnost nesou odpovědnost zaměstnanci v následujících pozicích:

* xxx doplnit
* př. Odpovědná osoba: Bezpečnostní ředitel pro utajované informace

**2.1 Povinnosti zajistit bezpečnost chráněných údajů vyplývající pro společnost ze ZEKu (§ 88 odst. 1, 2, 4 a 5, § 88a odst. 1 a 2):**

§ 88

(1) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen

a) zajistit popřípadě, pokud sám nezajišťuje veřejnou komunikační síť, na základě písemné dohody v součinnosti s příslušným podnikatelem zajišťujícím veřejnou komunikační síť, technicky a organizačně bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob v souladu se zvláštním právním předpisem, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob při poskytování této služby,

b) zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací podle písmene a) vnitřní technicko-organizační předpis;

ochranu údajů a důvěrnost komunikací zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany,

c) informovat dotčené účastníky o specifickém riziku porušení bezpečnosti sítě ve vztahu k ochraně údajů podle písmene

a), a pokud toto riziko přesahuje rozsah jím přijímaných opatření, je povinen účastníky informovat i o veškerých možnostech docílení nápravy, včetně souvisejících nákladů,

d) vytvořit vnitřní postupy pro vyřizování žádostí o přístup k osobním údajům uživatelů; na žádost Úřadu pro ochranu osobních údajů mu podnikatelé poskytující veřejně dostupnou službu elektronických komunikací poskytnou informace o těchto postupech, počtu přijatých žádostí, o právním odůvodnění těchto žádostí a o jejich zodpovězení.

(2) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen předložit Úřadu na jeho vyžádání předpis uvedený v odstavci 1 písm. b). Zjistí-li Úřad, že je předpis uvedený v odstavci 1 písm. c) v rozporu s tímto zákonem, sdělí tuto skutečnost bezodkladně dotčenému podnikateli a stanoví mu přiměřenou lhůtu k odstranění nedostatků.

(3) Úřad je, po předchozím vyžádání předpisu uvedeného v odstavci 1 písm. b), oprávněn u podnikatelů poskytujících veřejně dostupnou službu elektronických komunikací kontrolovat dodržování tohoto předpisu, s výjimkou kontroly plnění povinností týkajících se ochrany osobních údajů.

(4) V případě porušení zabezpečení osobních údajů se postupuje podle obecného nařízení o ochraně osobních údajů.

(5) Úřad pro ochranu osobních údajů je oprávněn po prošetření vzniklého stavu porušení zabezpečení osobních údajů uložit podnikateli poskytujícímu veřejně dostupnou službu elektronických komunikací povinnost, aby dotčenou fyzickou osobu o tomto porušení informoval, pokud již tak neučinil sám.

(6) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací vede pouze pro účely přezkumu plnění povinností podle odstavců 4 a 5 přehled porušení zabezpečení osobních údajů, včetně informací o okolnostech porušení, jeho dopadech a opatření přijatých k nápravě stavu. Prováděcí právní předpis může stanovit podrobnější podmínky, za nichž je podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen oznámit porušení zabezpečení osobních údajů, formát tohoto oznámení a způsob, jakým se má oznámení učinit.

§ 88a

(1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna zajistit, aby provozní a lokalizační údaje uchovávané podle § 97 odst. 3 měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím, jako údaje podle § 88; tímto nejsou dotčeny povinnosti stanovené zvláštním právním předpisem34).

(2) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna zpracovat pro zajištění ochrany údajů podle odstavce 1 vnitřní technickoorganizační předpis; ochranu údajů zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany. Pro ochranu údajů podle tohoto ustanovení se ustanovení § 88 odst. 2 až 7 použijí obdobně.

**2.2 Poskytování služeb za krizových stavů dle §99**

**3 NAPLNĚNÍ POŽADAVKŮ ZÁKONA**

**3.1 Analýza bezpečnostních rizik**

Požadavky na bezpečnost (důvěrnost, dostupnost a integritu informací) a ochranu informací jsou v rámci společnosti stanoveny na základě periodicky prováděného hodnocení bezpečnostních rizik a na základě normativních a legislativních požadavků. V rámci těchto analýz jsou stanovovány úrovně hrozeb, které mohou jednotlivá aktiva ohrozit, a úrovně zranitelností jednotlivých aktiv vůči těmto hrozbám. Následně je vypočtena míra rizik a doporučena bezpečnostní opatření

na jejich pokrytí. Výstupy z analýz jsou využity pro určení priorit bezpečnosti informací a k plánování opatření a zdrojů na pokrytí nově identifikovaných bezpečnostních rizik.

Proces řízení rizik je v podmínkách společnosti definován ve směrnicích Řízení rizik a pracovním postupu Řízení rizik informační a kybernetické bezpečnosti.

V rámci přípravy na audit ISMS jsou závěry z analýz rizik, včetně dopadů spojených s možným únikem chráněných údajů shrnuty v těchto dokumentech:

 Rozhodnutí k organizaci, řízení rizik a správě ISMS

 Rozhodnutí o výstupech z přezkoumání ISMS.

Revize analýzy v rámci přípravy společnosti na periodické audity ISMS jsou prováděny každoročně.

Doplnit další rizika vyplývající z provedené analýzy

**3.2 Dopady narušení bezpečnosti**

Hodnocení dopadů narušení bezpečnosti je prováděno v souladu s metodikou doplnit Dopady jsou ohodnoceny vybranými respondenty – manažery informačních systémů / garanty aktiv prostřednictvím podrobných dotazníků v čem doplnit

Způsob stanovení velikosti dopadů, včetně hodnocení následků v případě narušení důvěrnosti chráněných údajů, je detailně popsán v dokumentu doplnit

Rozhodnutí k organizaci, řízení rizik a správě ISMS a v dalších navazujících výstupech vytvořených v rámci přípravy společnosti na periodické audity ISMS.

**3.3 Pokrytí identifikovaných rizik**

V případě, kdy jsou identifikovány bezpečnostní požadavky, je s využitím metodiky RIAN a v souladu doporučeními mezinárodně uznávaných standardů (např. ISO/IEC 27001:2013, ISO/IEC 27002:2013) nalezena vhodná sada opatření na pokrytí identifikovaných rizik.

Implementovaná opatření snižují riziko narušení bezpečnosti chráněných údajů na přijatelnou úroveň, opatření pokrývají oblast fyzické, administrativní, personální, komunikační a IT bezpečnosti. Detailní popis přístupu ke zvládání neakceptovatelných rizik je popsán v Rozhodnutí o výstupech z přezkoumání ISMS, a v dalších navazujících plánech zvládání rizik vytvořených v rámci přípravy společnosti na periodické audity ISMS. Detailní přehled implementovaných opatření přijatých v jednotlivých informačních systémech je dostupný v elektronické podobě ve schváleném dokumentu doplnit dle pravidel a dokumentace společnosti

V případě, kdy dojde k úniku chráněných údajů, je aktivován proces zvládání bezpečnostních incidentů a co nejrychleji přijata odpovídající bezpečnostní opatření, která mají za cíl zabránit dalšímu případnému šíření škod, zmírnit dopady narušení bezpečnosti a zabránit opětovnému výskytu incidentů. V případě porušení ochrany osobních údajů se postupuje podle doplnit dle dokumentace společnosti

**3.4 Zpracování chráněných údajů**

S ohledem na jejich velký počet je evidence systémů zpracovávajících a uchovávajících osobní, identifikační a provozní údaje vedena v elektronické podobě v předepsaných interních aplikacích

Doplnit dle pravidel společnosti

**3.5 Přístup třetích stran k chráněným údajům**

Přístup třetích stran k chráněným informacím je ošetřen na úrovni:

 organizačních opatření – směrnice Ochrana informací – zejména příloha č. 3, směrnice Zvláštní podmínky

zpracování jednotlivých kategorií chráněných informací, smlouvou o ochraně informací NDA;

 konkrétní způsoby ochrany chráněných informací – Ochrana informací;

 technická opatření – Bezpečnostní manuál pro uživatele a administrátory inf. systémů

V případě přístupu do interních systémů společnosti jsou zástupci třetích stran povinni dodržovat interní řídící dokumentaci doplnit další související dokumenty společnosti

**4 související dokumenty**

V následující tabulce je uveden přehled související řídící dokumentace společnosti. Doporučené ČTÚ:

001 Bezpečnostní politika

002 Managment kontinuity

003 Organizační řád

004 Pracovní řád

**005 Ochrana osobních, provozních a lokalizačních údajů, důvěrnosti komunikací dle §88**

006 Havarijní a krizové řízení, krizový štáb

007 Metodika fyzické ochrany budov

Doplnit dle obsahu dokumentace společnosti