59/2018

ZMLUVA
O ADMINISTRÁCII POČÍTAČOVEJ SIETE

Objednávateľ: Kultúrne centrum Údolia Bodvy a Rudohoria
Zastúpený: MA Michal Kupec
Sídlo: Hlavná 52, 045 01 Moldava nad Bodvou
IČO: 42 104 076
DIČ: 2022735627

/ďalej ako užívateľ/

a

Zhotoviteľ: Jozef Tóth – T – SOFT
Sídlo: Peder č. 107, 044 05 Peder
IČO: 41 941 161
DIČ: 1073336484
Zapísaný v Živnostenskom registri OÚ Košice-okolie
č. OŽP-C/2006/00280-2/CR1
č. živnostenského registra 830-11720
Bankové spojenie: VÚB, a.s.
Číslo účtu: 2178 3293 55 / 0200
IBAN: SK42 0200 0000 0021 7832 9355
BIC/SWIFT: SUBASKBX

/ďalej ako administrátor/

Základné pojmy

Informačné systémy (IS) – súhrn technických prostriedkov, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením.

Informačné technológie (IT) – hardwarové a softwarové prostriedky, metódy a spôsoby určené na prenos, spracovanie a uchovanie informácií.

Užívateľský účet – (prihlasovacie meno a heslo) slúži na identifikáciu užívateľa v informačných systémoch a počítačovej sieti, umožňuje správne priradenie pridelených užívateľských práv prihlásenému užívateľovi. S každým jednotlivým užívateľským účtom sú spojené prístupové práva, ktoré rozhodujúcim spôsobom definujú oprávnenie užívateľa pristupovať k zdrojom počítačovej siete.

Cudzia osoba – osoba, ktorá nie je zamestnancom firmy resp. organizácie. (napr. syn, dcéra, kamarát, atď. zamestnanca, klient firmy resp. organizácie, atď.)

Oprávnený užívateľ (resp. len užívateľ) – zamestnanec (a cudzia osoba), ktorému bol zriadený užívateľský účet a pridelené príslušné prístupové práva na vykonanie danej činnosti.

Nepovolaná osoba – zamestnanec (a cudzia osoba), ktorý nemá pridelené prístupové práva na vykonanie danej činnosti alebo operácie.

Sieťové prvky – zariadenia napr. osobný počítač, pracovná stanica, server, lokálna sieť (LAN), aktívny rozbočovač (HUB), prepínač (SWITCH), smerovač (ROUTER), FIREWALL, prístupový bod pre bezdrôtové spojenie (ACCESS POINT) a pod., vrátane príslušného programového vybavenia.

Pracovné dokumenty – všetky súbory, ktoré užívatelia informačného systému vytvorili alebo prevzali pre potreby plnenia pracovných povinností.

Správca siete – osoba, ktorá je v zmluvnom vzťahu a ktorého náplň práce je definovaná v Čl. 9 Práva a povinnosti administrátora, ďalej len „administrátor".

Čl. 1
Predmet zmluvy

Administrátor sa zaväzuje optimalizovať počítačovú sieť, jednotlivé pracovné stanice a bezpečnosť Internetového pripojenia podľa Čl. 7 Pripojenie počítača do siete, Čl. 10 Postupy zabezpečenia počítača.

Čl. 2
Čas plnenia

Administrátor mesačne alebo podľa potreby užívateľa, okolnosti prekontroluje určené počítače, pracovné stanice. Spraví aktualizácie operačných systémov, Internetového prehliadača, antivírového systému, proxy servera. Prekontroluje správnu funkčnosť antivírového systému, proxy servera, Internetového prehliadača. Konzultácia, administrácia na požiadanie užívateľa raz za mesiac je bezplatná.

Čl. 3
Cena

Dohodnutá paušálna cena za administráciu počítačovej siete je 16,60 EUR /počítač/mesiac. Administrácia 4 počítačov mesačne: 4 x 16,60 EUR = 66,40 EUR. Vo výnimočných prípadoch celková fakturovaná suma sa môže zmeniť na základe nad rámec realizovaných prác.

Čl. 4
Práva a povinnosti užívateľov

1. Používanie hesiel

Každý užívateľ IS a počítačovej siete sa musí identifikovať - musí sa prihlásiť príslušným užívateľským menom a heslom. Autorizácia užívateľa v informačnom systéme môže byť viac úrovňová, pri prihlásení sa do IS a počítačovej siete, pred vstupom do určitej aplikácie, prípadne pred vykonaním určitej činnosti v rámci aplikácie. Na každej úrovni je vhodné používať iné heslo (heslá pre prihlásenie do siete a do konkrétnych aplikácií môžu byť rôzne). Meno užívateľa a prvotné heslo je užívateľovi pridelené administrátorom alebo aplikácie. Heslo je možné zmeniť. Správu hesiel vykonáva administrátor. Heslo musí obsahovať minimálne 6 znakov, kombináciu veľkých a malých písmen, číslic a špeciálnych znakov. (napr.: 89JahodaAQ) Kombinácia znakov tvoriacich heslo nesmie byť jednoducho dešifrovateľná. Je nevhodné používať mená a priezviská užívateľov, ich rodinných príslušníkov, dátumy narodení a pod. **Za utajenie hesla zodpovedá užívateľ.** Heslá nesmú byť voľne dostupné, napr. vedľa počítača, pod klávesnicou, na stole a pod. Každý užívateľ je zodpovedný za neoprávnené sprístupnenie svojho hesla inej osobe, následne i za jeho zneužitie. V prípade straty hesla užívateľ je povinný informovať administrátora počítačovej siete a zabezpečiť výmaz hesla, aby nemohlo dôjsť k jeho zneužitiu inou neoprávnenou osobou. V prípadoch keď je žiaduce zabezpečenie zvýšenej ochrany dát alebo prístup do IS prostredníctvom pracovnej stanice je potrebné používať zaheslovaný šetrič obrazovky.

Kľúčové heslá potrebné na zabezpečenie prevádzky IS a počítačovej siete sú uložené na predpísaných formulároch.

2. Používanie prostriedkov IS a počítačovej siete

Základnými prostriedkami IS a počítačovej siete, ktoré je možné používať pri plnení pracovných povinností sú:

a) pracovná stanica, ktorá bola zamestnancovi pridelená, resp. iný počítač, ktorý je zamestnanec oprávnený používať,
b) nainštalované programové vybavenie,
c) sieťové služby dátových serverov,
d) výpočtová kapacita počítačových systémov pri používaní sieťových aplikácií,
e) elektronická pošta E-mail,
f) pripojenie do globálnej siete Internet.

3. Zásady používania prostriedkov IS a počítačovej siete

a) Užívateľ nesmie svojvoľne meniť konfiguráciu pracovných staníc a počítačov.
b) Užívateľ nesmie počítače odpájať prípadne sám zapájať do počítačovej siete.
c) Užívateľ nesmie k počítačom pripájať ďalšie zariadenia, premiestňovať počítače, ani nijakým iným spôsobom zasahovať do ich hardwarového a softwarového vybavenia.
d) Užívateľ nesmie sám inštalovať akékoľvek programy, nesmie používať a šíriť nelegálne programové vybavenie, nesmie kopírovať a distribuovať nainštalované programy a operačné systémy, ich časti, súvisiacu dokumentáciu a manuály.
e) Všetky zmeny v konfigurácii počítača a ostatného technického vybavenia môžu byť vykonávané len spolu s administrátorom.
f) Pracovné dokumenty sa na pridelenom počítači odporúča ukladať do preddefinovaných priečinkov alebo do pracovného priečinka „Moje dokumenty", resp. „Dokumenty". **Každý užívateľ je zodpovedný za zálohovanie vytvorených pracovných dokumentov (má povinnosť ukladať ich na pridelené externé pamäťové médium, resp. do prideleného priečinka na sieťovom disku, na lokálnom disku, atď.).**
g) Užívateľ je povinný vo svojom počítači i na sieti udržiavať poriadok v priečinkoch, rušiť nepotrebné súbory a dokumenty, zbytočne nevytvárať prázdne priečinky, ich chaotické kópie a pod.
h) Užívateľ využíva pridelené výpočtové prostriedky, počítačovú sieť, pridelenú elektronickú adresu (E-mail) a pripojenie do Internetu na plnenie úloh súvisiacich s jeho pracovným zaradením.
i) Každý užívateľ je povinný uposlúchnuť výzvu administrátora na ukončenie práce v počítačovej sieti. V prípade opakovanej výzvy administrátora a jej následného neuposlúchnutia, je administrátor oprávnený ukončiť prihlásenie užívateľa na strane servera. *Poznámka: Administrátor má v prípade havarijného stavu právo na odstavenie prevádzky siete na dobu potrebnú k uvedeniu siete do štandardnej prevádzky aj bez predchádzajúceho upozornenia.*
j) Pri opustení pracovnej stanice (PC) pripojenej na počítačovú sieť je užívateľ povinný sa zo siete odhlásiť alebo zabezpečiť, aby nebolo možné pracovať pod jeho identitou (napr. zaheslovaním šetriča obrazovky).
k) Žiaden užívateľ nesmie zneužiť nedbanlivosť iného užívateľa na to, aby používal PC, IS alebo počítačovú sieť pod cudzou identitou.
l) Užívateľ nesmie vedome a zbytočne rušiť prácu ostatných užívateľov počítačovej siete, obmedzovať jej chod a výkonnosť.

m) Každý oprávnený užívateľ je povinný dodržiavať bezpečnostné opatrenia vyplývajúce z bezpečnostnej politiky, definovanej v „Bezpečnostnom projekte".
n) Počítače musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.
o) Užívateľ môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp dodávateľa zariadenia.
p) Užívateľ nesmie znižovať životnosť pracovných staníc hrubým zaobchádzaním a ich znečisťovaním.
q) V blízkosti počítačov je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie a podobne).
r) Čistenie povrchu počítačov od prachu je v kompetencii používateľa pracovnej stanice.

4. Používanie elektronickej pošty na plnenie pracovných povinností

Pri používaní elektronickej pošty platia rovnaké pravidlá ako pri obyčajnej pošte (rešpektovanie listového tajomstva). Elektronická pošta má charakter lístkov a pohľadníc, ktoré sa zasielajú bez obalu. Zabezpečenie dôvernosti a utajenia sa realizuje nadstavbovými prostriedkami (napr. zakódovaním správy tak, aby ju mohli odkódovať a prečítať len oprávnení príjemcovia).

Je zakázané:

a) používať elektronickú poštu spôsobom, ktorý je v rozpore s pracovným poriadkom a s platnou legislatívou Slovenskej republiky,
b) obťažovať ostatných užívateľov zasielaním nevyžiadaných informácií, šírením počítačových vírusov, šírením tzv. „reťazových listov" a poplašných správ (hoax) typu „Dieťa s leukémiou" alebo „vírus, ktorý nedokáže odhaliť žiaden antivírový program" a pod., na konci so žiadosťou „pošli to všetkým známym",
c) zasielanie hromadných nevyžiadaných oznamov (okrem organizačných útvarov ktoré na to majú povolenie),
d) používanie vulgárnych a znevažujúcich výrazov v komunikácii,
e) posielanie a otváranie k elektronickej pošte pripojených súborov, ktoré by mohli nejakým spôsobom ohroziť alebo poškodiť prevádzku IS a počítačovej siete, trvale alebo dočasne znížiť ich výkonnosť alebo ohroziť ich bezpečnosť.

Príjemca elektronickej pošty potvrdí odosielateľovi jej prevzatie vtedy, ak o to odosielateľ v texte správy výslovne žiada.
Používanie špeciálnych zariadení akými sú scanner, CD a DVD napaľovačka, prenosné USB pamäte a pod. je možné iba v súlade s bezpečnostnou politikou.
Užívatelia majú z dôvodu plnenia pracovných povinností zabezpečený prístupu na Internet. Pri vyhľadávaní informácií je zakázané navštevovať pornografické a hackerské stránky, ktoré predstavujú pre Internetový prehliadač hrozbu nielen vírusovú. Zasielanie nevyžiadanej elektronickej pošty - SPAM je v SR zakázané, viď §3 ods. 6 zákona č. 147/2001 Z. z. o reklame a o zmenách a doplnení niektorých zákonov. Pretože sa väčšinou jedná o propagáciu rôznych komerčných firiem a pornografických stránok, je zakázané ju po prevzatí otvárať a klikať na linky v nej uvedené. O tejto skutočnosti je potrebné informovať administrátora.
Každý užívateľ absolvuje zaškolenie a písomne potvrdí, že je oboznámený s pravidlami používania IS a počítačovej siete a, že ich bude dodržiavať.

Čl. 5
Ochrana údajov

(1) Užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva, alebo privilegovaný stav, ktorý mu nebol pridelený administrátorom. Pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť administrátorovi. Užívateľ nesmie vykonávať takú činnosť, ktorá by ostatným užívateľom bránila v riadnom používaní siete, napr. šírenie počítačových vírusov, alebo pokusy o neoprávnený prístup k prvkom IS a počítačovej siete.

(2) Užívateľ sa nesmie pokúšať získať prístup k chráneným informáciám a dátam (resp. dátovej komunikácii) iných užívateľov. Všetky dáta obsiahnuté v zariadeniach siete sú považované za dôverné, pokiaľ nie je explicitne uvedené alebo z ich povahy zrejmé (napr. obsah verejnej web stránky), že sú určené pre všeobecné a neobmedzené použitie.

(3) Užívateľ nesmie napomáhať iným osobám pri získavaní prístupových práv alebo privilegovaných stavov, ktoré im neboli pridelené administrátorom, ani pri získavaní prístupu k chráneným informáciám a dátam iných užívateľov.

(4) Užívateľom je zakázané neodôvodnené sťahovanie a prijímanie súborov (hlavne súbory s príponami: **.EXE, .COM, .SCR, .REG, .CPL, .DLL, .SYS, .VBE, .VBS, .VXD, .BAT**) z Internetu, z príloh časopisov CD a DVD a z iných nedôveryhodných zdrojov akými sú napr. nelegálne kópie FD, CD a DVD a rôzne DEMO, TRIAL, BETA, FREEWARE, SHAREWARE, POSTCARDWARE verzie programov a pod. Výnimka je povolená len od administrátora alebo na základe pracovnej náplne užívateľa.

(5) V prípade úniku alebo podozrenia z úniku informácií z IS a počítačovej siete sú všetci zamestnanci povinní oznámiť túto skutočnosť osobe poverenej výkonom dohľadu nad ochranou osobných údajov.

(6) Prostriedky výpočtovej techniky na ktorých sú údaje z informačnej bázy dát, pamäťové médiá s údajmi a programami (napr. CD, DVD) a výstupné tlačové zostavy, musia byť mechanicky zabezpečené pred prístupom nepovolaných a cudzích osôb (napr. umiestnením v uzamykateľných priestoroch).

(7) Inštalačné médiá (napr. MS-WINDOWS®, MS-OFFICE® a pod.) a médiá so zálohami dát z informačných systémov (CD, DVD) musia byť evidované a uložené v priestoroch, v ktorých budú zabezpečené pred znehodnotením a neoprávneným použitím.

(8) Všetci zamestnanci, ktorí pracujú s osobnými a dôvernými údajmi sú povinní riadiť sa ustanoveniami zákonov č. 18/2018 Z.z. a 540/2001 Z.z. Každý zamestnanec má povinnosť zachovávať mlčanlivosť o osobných a dôverných údajoch o ktorých sa dozvedel pri plnení pracovných povinností a o tých, ktoré v záujme zamestnávateľa nie je možné oznamovať iným osobám. Povinnosť zachovávať mlčanlivosť trvá aj po skončení pracovného pomeru, obdobného pracovného alebo zmluvného vzťahu. Spracovanie osobných a dôverných údajov na počítačoch mimo pracovísk je zakázané.

Čl. 6
Ochrana osobných údajov

Administrátor pri spracúvaní osobných údajov postupuje v súlade so zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi prepismi a rešpektuje príslušné povinnosti určené objednávateľom. Administrátor nesmie spracúvané osobné údaje využiť pre osobnú potrebu, či potrebu inej osoby, ani sprístupniť alebo na iné, než služobné/pracovné účely. Administrátor je povinný zachovať mlčanlivosť o osobných údajoch s ktorými príde do styku.

Čl. 7
Pripojenie počítača do siete

(1) Do siete môže byť zapojený počítač, ktorý je vedený v evidencii majetku firmy resp. organizácie a má pridelené inventárne číslo. Počítače, ktoré nie sú evidované v majetku firmy resp. organizácie (napr. PC cudzích osôb), môžu byť pripojené do siete len so súhlasom administrátora.

(2) Do siete môže počítač pripojiť len administrátor.

(3) Počítače v sieti sú určené nasledovnými identifikačnými údajmi:
a) IP adresa
b) MAC adresa
c) Meno a priezvisko zamestnanca, ktorý zodpovedá za daný počítač
d) Inventárne číslo (u počítača cudzích osôb súhlas administrátora)

(4) Počítač ktorému chýba niektorý z týchto 4 atribútov, nemôže byť zapojený v sieti.

Čl. 8
Súvisiace predpisy

Zákon č. 18/2018 Z.z. o ochrane osobných údajov (GDPR)
platnosť: 30.01.2018, účinnosť: 25.05.2018, zdroj: Zbierky zákonov

Zákon č. 540/2001 Z.z. o štátnej štatistike,
platnosť: 20.12.2001, účinnosť: 01.01.2002, zdroj: Zbierky zákonov.

Zákon č. 185/2015 Z.z. Autorský zákon,
platnosť: 05.08.2015, účinnosť: 01.01.2016, zdroj: Zbierky zákonov.

Zákon č. 300/2005 Z.z. Trestný zákon,
platnosť: 02.07.2005, účinnosť: 01.01.2006, zdroj: Zbierky zákonov

Čl. 9
Práva a povinnosti administrátora

Správa počítačovej siete sa stáva v dobe prudkého rozvoja Internetu zložitejšou a náročnejšou úlohou, než bola kedykoľvek predtým. Administrátor má na základe svojej kvalifikácie predpoklady na výkon tejto funkcie. (príloha č. 5)

(1) Administrátor zodpovedá za prevádzku siete, jej technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete.
(2) Administrátor je prvým konzultantom pre všetkých zamestnancov v oblasti funkčnosti siete a pri následnom riešení poruchových stavov.
(3) Administrátor je kontaktnou osobou pri riešení problémov komunikácie v sieti.
(4) Administrátor zodpovedá za:
    a) technickú a systémovú správu lokálnej siete na určených počítačoch pripojených do LAN,
    b) správne nastavenie komunikačných parametrov počítačov pripojených na LAN,
    c) dodržiavanie podmienok pripojenia podľa **Čl. 7 Pripojenie počítača do siete**,
    d) okamžité odpojenie od počítačovej siete takého počítača, ktorý porušuje pravidlá pripojenia, alebo správania sa v sieti,
    e) prešetrenie príčin porušovania pravidiel a ich odstránenie.
(5) Administrátor nezodpovedá:
    a) za užívateľov ktorí nerešpektujú, ignorujú **Čl. 4 Práva a povinnosti užívateľov, Čl. 5 Ochrana údajov, Čl. 7 Pripojenie počítača do siete, Čl. 8 Súvisiace predpisy, Čl. 9 Práva a povinnosti administrátora**
    b) za porušenie zákona č. 185/2015 Z.z. Autorský zákon
    c) za pharming a nefunkčnosť vonkajších DNS serverov,
    d) za legálne a nelegálne programy používané vo firme, resp. v organizácie,
    e) za funkčnosť alebo nefunkčnosť softvérov používaných vo firme, resp. v organizácie,
    f) za audit softvérov,
    g) za archiváciu údajov,
    h) za nefunkčnosť Internetu pôsobené poskytovateľom (ISP),
    i) za nefunkčnosť vonkajších elektronických služieb ako napr.: webové stránky, E-mail, Internet banking, atď.
    j) za router, switch, firewall, kábeláž ktorý už bol nainštalovaný pred administráciou siete a administrátor nemá k tomu prístup,
    k) za nesprávnu konfiguráciu routera, firewalla, proxy servera ktorý už bol nainštalovaný pred administráciou siete a administrátor nemá k tomu prístup.
(6) Pri mimoriadne vážnych ohrozeniach siete môže odpojiť z komunikácie celú sieť, resp. jeho časť na nevyhnutne potrebnú dobu.
(7) Správca siete prideľuje IP adresy z rozsahu, ktorý má k dispozícii a vedie evidenciu, vrátane mena zodpovedného zamestnanca, udržuje ich v aktuálnom stave.
(8) Sleduje stav siete a podľa potreby informuje jej užívateľov. Pozná a používa monitorovacie a diagnostické techniky.
(9) Vykonáva analýzu bezpečnostných incidentov zo systému firewallu, antivíru a pod.
(10) Užívateľom siete poskytuje poradenské služby a navrhuje potrebu absolvovania školení na rozvoj zručností, ktoré by zvyšovali kvalifikáciu užívateľov siete, čím napomáha optimalizovať jej prevádzku a správu.
(11) Vedie dokumentáciu o počítačovej sieti a navrhuje potrebu jej inovácie.

Čl. 10
Postupy zabezpečenia počítača

(1) Zablombovanie krytu počítača resp. pracovnej stanice.

(2) Nastaviť heslo pre prístup do BIOSu.

(3) Nastaviť štartovanie počítača iba z pevného disku. Nastaviť prvotný HDD-0 ako boot. Zrušiť prvotný boot z FD/CD/DVD/LAN/USB.

(4) Zapísať štandardný BOOT LOADER na HDD-0. (mazanie možného BOOT vírusa)

(5) Nastaviť v BIOSe ochranu MBR proti prepísaniu. (ochrana proti BOOT vírusu)

(6) Pri použití operačného systému Windows® NT/2000/XP/Vista/Win7/Win8.x/Win10 použiť súborový systém NTFS. Na pevných diskoch pod kapacitou 2TB používať MBR partíciu namiesto GPT partície.

(7) Vytvorenie administrátorského konta, vytvorenie užívateľských kont.

(8) Zapnúť integrovaný firewall v operačnom systéme, povoliť odpoveď ICMP [0]Echo Reply na žiadosti ICMP [8]Echo Request.

(9) Len na žiadosť užívateľa Internetový prístup riešiť podľa prílohy č. 4. V tomto prípade pre jednotlivé programy ktoré potrebujú Internetové pripojenie nastaviť prístup cez proxy server s overovaním, pre Internetový prístup nepoužívať gateway, nevyplniť predvolenú bránu na jednotlivých pracovných staniciach, iba na centrálnom počítači. (podľa prílohy č. 4).

(10) Vypnúť sieťovú službu počúvajúcu na porte TCP135 – vzdialené volanie procedúr.

(11) Vypnúť sieťovú službu počúvajúcu na porte TCP5000 – Universal Plug and Play.

(12) Vypnúť službu vzdialená pracovná plocha, vzdialená pomoc, vzdialený register.

(13) Vypnúť kuriérsku službu messenger.

(14) Vypnúť službu zdieľanie súborov a tlačiarní, ak nie je využitá. V prípade potreby povoliť iba pre daný počítač s filtrovaním cez integrovaný firewall pre lokálnu sieť.

(15) Vypnúť Full Raw Sockets. Platí pre operačné systémy Windows® NT/2000/XP.

(16) Vypnutie zbytočných procesov pri spustení operačného systému. (napr. extra ovládače grafických a zvukových kariet, monitorovacie softvéry iných aplikácií, atď.)

(17) Inštalovanie antivírového systému schopnosťou HTTP, SMTP, POP3 kontroly.

(18) Nastaviť antivírový systém tak, aby skontroloval BOOT sektory, všetky (*.*) súbory pri otváraní, vytváraní, spúšťaní. Nastaviť heuristickú analýzu. Nastaviť HTTP, SMTP, POP3 kontrolu. Nastaviť automatické aktualizácie antivírového systému.

(19) Z bezpečnostných dôvodov je odporúčané používať nasledovné softvéry: Internetový prehliadač - Mozilla® Firefox®, E-mailový klient - Mozilla® Thunderbird®, Proxy server - FreeProxy®.

Čl. 11
Záverečné ustanovenia

(1) Všetci užívatelia IS a počítačovej siete sú povinní dodržiavať túto zmluvu, ustanovenia súvisiacich právnych noriem a ďalšie pravidlá, pokyny a platné predpisy.

(2) Táto zmluva je záväzná pre všetkých užívateľov IS a počítačovej siete.

(3) Administrátor pri spracúvaní osobných údajov postupuje v súlade so zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi prepismi a rešpektuje príslušné povinnosti určené objednávateľom. Administrátor nesmie spracúvané osobné údaje využiť pre osobnú potrebu, či potrebu inej osoby, ani sprístupniť alebo na iné, než služobné/pracovné účely. Administrátor je povinný zachovať mlčanlivosť o osobných údajoch s ktorými príde do styku.

(4) Zmluva sa uzatvára na dobu určitú na 1 rok a platnosť a účinnosť nadobúda dňom podpisu obidvoma zmluvnými stranami.

(5) Platnosť a účinnosť tejto zmluvy zaniká dňom ukončenia zmluvy. Povinnosť mlčanlivosti trvá aj po ukončení platnosti a účinnosti tejto zmluvy.

(6) Zmluvné strany sa dohodli, že text tejto zmluvy bude utajené pred tretími stranami a predstavuje dôverné informácie. V prípade zverejnenia zmluvy nezverejniť pečiatky a podpisy v tejto zmluve.

(7) Zmeny a dodatky tejto zmluvy vyžadujú písomnú formu.

(8) Neoddeliteľnou súčasťou tejto zmluvy sú:
- príloha č. 1 – Vymedzenie niektorých odborných pojmov (5 strán)
- príloha č. 2 – Ako funguje predvolene nastavený FIREWALL? (1 strana)
- príloha č. 3 – Menej bezpečné riešenie Internetového prístupu (1 strana)
- príloha č. 4 – Bezpečnejšie riešenie Internetového prístupu (1 strana)
- príloha č. 5 – Osvedčenie: Jozef Tóth – správca počítačových systémov – kópia (1 strana, podpisy boli odstránené z osvedčenia)
- príloha č. 6 – Osvedčenie: Jozef Tóth – Zákon o ochrane osobných údajov – kópia (1 strana, podpis lektora bol odstránený z osvedčenia)

(9) Strany prehlasujú, že túto zmluvu prečítali a zhodne porozumeli jej obsahu, ktorý zodpovedá ich skutočnej, vážnej a slobodnej vôli, na dôkaz čoho pripájajú svoje podpisy.

(10) Táto zmluva je vyhotovená v 2 exemplároch, z ktorých každá má platnosť originálu.

(11) Táto zmluva obsahuje 20 strán spolu s prílohami.

V Moldave nad Bodvou, dňa: 07.05.2019

Jozef Tóth -T- SOFT
044 05 Peder 107
IČO:41 941 161 DIČ:1073336484
tel.: 0904 154 270
Živ. vyd. OÚ Ke-okolie
ROŽP-C/2006/00280-2/CR1, č.živ. reg. 830-11720

Objednávateľ

Zhotoviteľ