Základní škola a mateřská škola Neslovice,
okres Brno – venkov, příspěvková organizace

Hlavní 71, 664 91 Neslovice

Směrnice

„Bezpečnost ICT“

V Neslovicích 01.09.2020

Základní škola a mateřská škola Neslovice,
okres Brno - venkov,
příspěvková organizace
Tel.: 739 575 938
IČ: 709 99 503

.....
Mgr. Lenka Odehnalová
ředitelka ZŠ a MŠ

Za účelem naplnění Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení") a zákona č. 110/2019 Sb., o zpracování osobních údajů, se vydává tato směrnice:

Článek 1
Úvodní ustanovení

1. Směrnice stanovuje bezpečnostní pravidla pro zpracování, uchování a předávání dat Základní škola a mateřská škola Neslovice, okres Brno – venkov, příspěvková organizace, obsahující osobní údaje v souladu s požadavky obecného nařízení.
2. Směrnice je platná pro všechny zaměstnance Základní škola a mateřská škola Neslovice, okres Brno – venkov, příspěvková organizace (dále jen „organizace").
3. Bezpečnostní pravidla, definovaná touto směrnicí, jsou platná pro zpracování jakýchkoliv dat včetně osobních údajů ve všech operačních systémech a aplikacích, které jsou ve správě organizace a provozované buď na výpočetní technice, nebo na technice organizace a aplikacích poskytnutých smluvním dodavatelem.
4. **Organizace je coby zaměstnavatel oprávněna k monitoringu užívání informačních a komunikačních technologií na pracovišti prostřednictvím auditních záznamů používaných aplikací, informací o využití elektronické pošty, obsah zpráv pracovní povahy a statistiky navštívených webových stránek, z důvodu zajištění kybernetické bezpečnosti a kontroly pracovní činnosti zaměstnance.**

Článek 2
Základní pojmy

1. **Active Directory** – řešení adresářových služeb pro správu síťových prostředků. Active Directory využívají administrátoři počítačových sítí pro různé účely. Nastavují za jeho pomoci pravidla a politiku sítě, instalují programy na veliké množství PC stanic zároveň či řeší kritické situace v síti.
2. **Administrátor** – osoba pověřená správou jednoho, nebo více ICT zařízení, která je schválena ředitelem organizace a má nejvyšší úroveň oprávnění pro ICT zařízení ve své správě.
3. **Administrátorský účet** – uživatelský učet, jenž má nevyšší možná oprávnění v rámci daného operačního systému nebo aplikace.
4. **Aplikace** – programové vybavení výpočetní techniky organizace (např. MS Word).
5. **Cloud** - externí internetové datové uložiště (např. One Drive, Google drive, Dropbox apod.).
6. **Datová skříň** – standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů, zajišťující základní fyzickou bezpečnost.
7. Fyzická bezpečnost – znamená používání fyzických a technických ochranných opatření k zamezení neoprávněného přístupu k majetku a informacím organizace.
8. Garant aplikace – zaměstnanec odpovědný za konkrétní aplikaci. Garant aplikace je odborný zaměstnanec se znalostí dané aplikace. Plně rozhoduje o požadavcích na přístup k dané aplikaci, rušení přístupových oprávnění a přezkoumání přístupových oprávnění.

Pravidelně komunikuje se správcem ICT ohledně způsobů nastavení a zabezpečení konkrétní aplikace. Společně se správcem ICT je klíčovou rolí v zabezpečení dat organizace.

9. Hardware – označuje veškeré fyzicky existující technické vybavení výpočetní techniky či síťových prostředků.

10. Operační systém – základní programové vybavení počítače (tj. software), který je zaveden do paměti počítače při jeho startu a zůstává v činnosti až do jeho vypnutí (např. MS Windows 10).

11. Osobní údaj – veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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.

12. Počítačová síť organizace – síťové prostředky a výpočetní technika ve správě a/nebo v majetku organizace, které realizují spojení a výměnu informací.

13. Pověřenec pro ochranu osobních údajů – zaměstnanec organizace nebo smluvní externí subjekt pověřený plněním povinností v oblasti zpracování a ochrany osobních údajů ve smyslu kapitoly IV, oddílu 4 obecného nařízení (dále také jen „pověřenec").

14. Provozní deník – písemný dokument nebo elektronický soubor, který obsahuje všechny činnosti, které při správě počítačové sítě provádí správce ICT.

15. Přístupový údaj – sada informací potřebných pro přihlášení do operačního systému nebo aplikace. V základní podobě jsou tvořeny uživatelským jménem a heslem.

16. Režimová opatření – ucelený soubor opatření, pokynů, příkazů, zákazů a omezení představující soupis instrukcí pro vstup, odchod, pohyb v objektu a přístup k informacím organizace.

17. Síťové prostředky – technická zařízení používaná k zajištění provozu, správy a bezpečnosti sítě organizace. Jedná se zejména o Routery, servery, switche, firewall apod.

18. SLA – Service Level Agreement – dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby.

19. Správce ICT – osoba odpovědná za provozování a správu počítačové sítě a prostředků ICT organizace. Disponuje nejvyššími administrátorskými účty k operačním systémům a některým aplikacím. Společně s garantem aplikace je klíčovou rolí v zabezpečení dat organizace.

20. Uživatel – zaměstnanec využívající výpočetní techniku organizace.

21. Uživatelské jméno – jednoznačný identifikátor uživatele v systému. Jedná se o unikátní jméno zpravidla složené z písmen (případně i číslic).

22. Uživatelský účet – jednoznačná identifikace uživatele v rámci operačního systému nebo aplikace. Uživatelský účet umožňuje plnou práci, ale bez možnosti instalovat aplikace do výpočetní techniky nebo měnit nastavení operačního systému nebo aplikace. Uživatelský účet se standardně skládá z uživatelského jména a hesla.

23. VPN – Virtuální privátní síť (zkratka VPN, anglicky Virtual Private Network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě.

24. Výpočetní technika – soubor počítačů, notebooků, tabletů nebo smartphonů organizace. Obecně všech zařízení, která disponují vlastním operačním systémem.

25. Zvláštní kategorie údajů – osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Článek 3

Organizace bezpečnosti

1. Ředitel organizace je odpovědný za ustanovení zaměstnanců do jednotlivých rolí, ve kterých budou odpovědni za řízení bezpečnostních požadavků na ochranu osobních údajů. Jedná se především o ustanovení rolí:

a) pověřence pro ochranu osobních údajů,

b) správců ICT, a

c) jednotlivých garantů aplikací.

2. Ředitel organizace schvaluje přidělení lokálních administrátorských účtů vybraným zaměstnancům.

3. Organizace identifikuje dodavatele aplikací a služeb ICT s možností přístupu k datům organizace a uzavře s nimi smlouvy, příp. dodatek smlouvy o zpracování osobních údajů v souladu s požadavky čl. 28 GDPR.

4. Ředitel je odpovědný za zajištění pravidelného školení všech zaměstnanců v oblasti bezpečnosti informací.

5. Školení musí obsahovat následující oblasti: tvorba a správa hesel, ochrana neobsluhovaných zařízení, ochrana dat při jejich sdílení, ochrana přenosných zařízení při práci mimo prostory organizace, pravidla ukládání a zálohování dat, nejčastější typy úniku informací, vzorové phishingové e-maily, co vše může být bezpečnostním incidentem, procesy hlášení bezpečnostních událostí/incidentů a další oblasti dle potřeby.

Článek 4

Bezpečnostní pravidla uživatelů

Zaměstnanci jsou povinni dodržovat následující bezpečnostní pravidla při zpracovávání osobních údajů:

1. Svěřenou výpočetní techniku využívají pouze pro plnění pracovních povinností.

2. Dodržují stanovené zásady pro tvorbu přístupového hesla k operačním systémům a/nebo aplikacím.

3. Při prvním přihlášení k operačním systémům anebo aplikacím, si musí změnit heslo zadané správcem ICT.

4. Zachovávají jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají.

5. Při přihlašování k operačním systémům a/nebo aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou.

6. V případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní.

7. Před opuštěním pracoviště, i krátkodobém, zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením (např. pomocí kláves □+L nebo ctrl+alt+del).

8. Při používání přenosné výpočetní techniky a datových nosičů (notebooků, flash disků, externích HDD, DVD apod.) mimo prostory organizace:

a) nepředávají tuto techniku a nosiče třetím osobám (ani rodinným příslušníkům),

b) učiní všechna dostupná opatření která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),

c) nepoužívají výpočetní techniku na veřejných místech pro práci s daty organizace,

d) nepřipojují se k nezabezpečeným, tzv. volným Wi-Fi sítím,

e) ztrátu či odcizení okamžitě nahlásí svému nadřízenému.

9. Neinstalují žádný software na výpočetní techniku organizace.

10. Nenavštěvují rizikové internetové stránky a neklikají na reklamní bannery na webových stránkách.

11. Důsledně ověřují doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), takovou zprávu neotvírají, nereagují na ní a tuto skutečnost neprodleně ohlásí správci ICT.

12. Nezasahují do výpočetní techniky a její konfigurace, vyjma situací, kdy toto bude vyžadováno přímo správcem ICT.

13. Odpovídají za zálohování dat na přidělené výpočetní technice dle postupů stanovených správcem ICT.

14. Netisknou data z aplikací organizace pro jiné než pracovní účely.

15. Pokud dojde k úniku, kompromitaci nebo ztrátě jakéhokoliv zařízení či dat obsahujících osobní údaje je každý zaměstnanec povinen neprodleně hlásit tento incident nadřízenému vedoucímu zaměstnanci, který tuto skutečnost hlásí neprodleně pověřenci pro ochranu osobních údajů.

Článek 5
Bezpečnostní pravidla správce ICT

1. Správce ICT je odpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v rámci počítačové sítě a na výpočetní technice organizace.
2. Správce ICT je v rámci organizace nejvyšším administrátorem výpočetní techniky a disponuje plnými přístupovými oprávněními ke všem síťovým prvkům a používané výpočetní techniky.
3. V případě potřeby může Správce ICT disponovat i vrcholnými administrátorskými oprávněními k používaným aplikacím. Předání vrcholných administrátorských oprávnění k používaným aplikacím může schválit jen ředitel organizace. O předání administrátorských oprávnění je proveden zápis.
4. Je povinen dodržovat následující bezpečnostní pravidla při plnění pracovních úkolů správce ICT:
   a) Zajišťuje bezpečné prostředí počítačové sítě organizace.
   b) Je odpovědný za správu všech síťových zařízení organizace (serverů, routerů, NAS apod.), nástrojů pro správu uživatelů, používání jen aktualizovaných programů a dalších nezbytných činností spojených s provozem výpočetní techniky organizace a zabezpečení sítě.
   c) Spolupracuje s organizací na tvorbě a aktualizaci analýzy rizik.
   d) Pro zaměstnance organizace připravuje a instaluje výpočetní techniku, kterou nastaví dle definovaných bezpečnostních požadavků (např. způsoby přihlášení, oprávnění uživatelského účtu, uzamykání počítače při neaktivitě apod.) a následně ji předává určeným zaměstnancům k použití.
   e) Spravuje antivirový systém na veškeré výpočetní technice organizace a to především:
      - provádí jeho instalaci,
      - kontroluje funkčnost aktualizací,
      - kontroluje výstupy programu.
   f) Operační systém a všechny aplikace ve správě organizace nastaví tak, aby uživatel byl vyzván ke změně hesla po 1. přihlášení a aby tento krok nebylo možné přeskočit.
   g) Na základě požadavku ředitele organizace zřizuje nebo ruší přístupy do operačních systémů organizace.
   h) Na základě požadavku garanta aplikace zřizuje nebo ruší přístupy do aplikace organizace.
   i) Zajišťuje fyzickou bezpečnost síťových zařízení (např. serverů, routerů, switchů apod.) a síťových datových úložišť, včetně zabezpečení záloh organizace dle pravidel daných touto směrnicí.

j) Poskytuje zaměstnancům organizace technickou podporu při využívaní výpočetní techniky.
k) Provádí kontrolní činnost k zajištění bezpečnostních požadavků na ochranu osobních údajů zpracovávaných ve výpočetní technice organizace.
l) Pravidelně alespoň 1x za 3 měsíce kontroluje bezpečné použití všech administrátorských účtů organizace a v případě zjištění jakéhokoliv možného problematického chování uživatele s administrátorským účtem (nedovolená instalace programů, změny v nastavení operačního systémů apod.) sám administrátorský účet dočasně omezí a bezodkladně informuje ředitele organizace.
m) Vede provozní deník, ve kterém zaznamenává všechny klíčové činnosti související se správou počítačové sítě organizace (např. bezpečnostní událost/incident, řízení přístupů (zřizování/změny/zrušení uživatelských oprávnění), přezkoumání přístupových oprávnění, vymazání účtů, zrušení přístupů (jak žádané, tak i mimořádné), zřízení přístupů, chyba v zálohování, obnova dat, změna nastavení zálohovacího procesu, aktualizace serverů, instalace softwaru apod.)
n) Provádí bezpečnou likvidaci datových nosičů organizace, zejména pak pevných disků, flash disků, paměťových karet, CD a DVD disků apod.
o) V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení, likvidace apod.), musí před odesláním nenávratně vymazat z pevného disku veškeré osobní údaje nebo musí vyjmout paměťová média.
p) Provádí zálohování zpracovávaných dat a klíčových síťových prostředků organizace tak, aby při selhání např. hlavního datového úložiště, bylo možné provést obnovu dat s minimální ztrátou uložených dat.

Článek 6
Řízení rizik

1. Ředitelem pověřená osoba provádí v pravidelných intervalech (alespoň jedenkrát za tři roky nebo při jakékoliv podstatné změně v konfiguraci sítě nebo systémů) analýzu rizik v souladu s metodikou pro analýzu rizik na základě požadavků čl. 24 a 32 GDPR.
2. Analýza rizik GDPR má za cíl určit možné hrozby a zranitelnosti při zpracování osobních údajů, včetně identifikace a stanovení rizik, která mohou vzniknout působením hrozeb na účely zpracování osobních údajů.

Článek 7
Řízení aktiv

1. Ředitelem pověřená osoba eviduje veškerý hardware (počítače, notebooky, mobilní telefony, flash a externí disky apod.), software a aplikace používané organizací.
2. Ke všem aplikacím jsou organizací určeni garanti aplikace. Jedna osoba může vykonávat garanta pro více aplikací.
3. Používání soukromých přenosných paměťových zařízení (externí pevné disky, flash disky a SD karty) pro ukládání nebo zpracování osobních údajů je zakázáno.
4. Paměťová zařízení, která potřebují zaměstnanci ke své práci, jsou evidována. Evidenci paměťových zařízení provádí správce ICT nebo jiná ředitelem pověřená osoba.
5. Veškerá výpočetní technika organizace disponuje aktuálním operačním systémem a aplikacemi, jež mají nastavené automatické aktualizace.
6. Při přidělení výpočetní techniky jinému zaměstnanci správce ICT provádí kompletní reinstalaci výpočetní techniky. Ředitel nebo jím pověřená osoba určí, jakým způsobem naložit s daty, která jsou na výpočetní technice uložena.

7. V případě vyřazení výpočetní techniky jsou paměťová zařízení softwarově skartována (přepsána náhodnými daty) nebo fyzicky zničena správcem ICT.

Článek 8

Řízení přístupů

1. Každý zaměstnanec disponuje přístupovými oprávněními dle pravidla „need to know", tedy takovými, které prokazatelně potřebuje ke své práci.
2. Každý zaměstnanec využívající výpočetní techniku organizace, používá pro připojení k operačním systémům a aplikacím jedinečné uživatelské jméno a heslo, které s nikým nesdílí.
3. Společné, projektové či jinak sdílené uživatelské účty k operačním systémům a aplikacím obsahující osobní údaje jsou zakázány.
4. Všem zaměstnancům organizace jsou k operačním systémům přidělovány jen základní uživatelské účty.
5. Administrátorské účty jsou striktně řízeny. Správce ICT na základě souhlasu ředitele organizace nastavuje přístupy tak, aby administrátorským účtem disponovali pouze zaměstnanci, kteří jej ke své práci prokazatelně potřebují (správci sítě, systému apod.).
6. Zaměstnanci s administrátorskými účty jsou prokazatelně seznámeni s faktem, že jsou majiteli administrátorského účtu a jsou si vědomi vyšších bezpečnostních a uživatelských nároků spojených s tímto typem účtu.
7. Administrátorské účty se všem oprávněným zaměstnancům vytvářejí jako samostatné uživatelské účty, které jsou jednoznačně odděleny od běžného účtu uživatele (např. za pomoci přidání předpony k uživatelskému jménu *admin_uživatelskéjméno*).
8. Zaměstnanci s administrátorskými účty jsou pro běžnou práci povinni používat standardní uživatelský účet. Administrátorský účet jsou oprávněni použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné. O provedených činnostech provedou záznam v provozním deníku.
9. Správce ICT vede seznamy zaměstnanců, kteří disponují administrátorskými účty. Ředitel organizace, ve spolupráci se správcem ICT, tyto seznamy přezkoumává z hlediska aktuálnosti a potřebnosti minimálně 1x do roka.
10. Garanti aplikací jsou odpovědní za řízení všech přístupových oprávnění zaměstnanců ke aplikacím ve své odpovědnosti.
11. Garanti aplikací sami řídí a nastavují jednotlivá přístupová oprávnění k aplikacím ve své odpovědnosti nebo ke konkrétnímu nastavení přístupových oprávnění pověří správce ICT.
12. Garanti aplikací spolupracují se správcem ICT na pravidelném přezkoumávání přístupových oprávnění do aplikací, které probíhá alespoň 1x do roka. O takovém přezkoumání je proveden záznam.
13. Při vzniku potřeby změnit přidělená přístupová oprávnění žádá přímý nadřízený zaměstnance:
    a) správce ICT v případě požadavků změny přístupů k síti, síťovým diskům apod. a
    b) garanta aplikace v případě požadavků změny přístupů k aplikacím.
14. V případě ukončení pracovního poměru zaměstnance jsou na základě pokynu ředitele veškerá přístupová oprávnění zaměstnance odebrána správcem ICT nebo příslušným garantem aplikace.

15. Na veškeré výpočetní technice organizace je nastaveno uzamykání uživatelského účtu do operačního systému max. po 10 min. jeho neaktivity. Pokud je to možné jsou všechny aplikace používající přihlašování uživatelů nastaveny stejně.
16. Minimální pravidla pro hesla uživatelů jsou stanovena následovně:
    a) minimální délka je 8 znaků, obsahující alespoň jednu číslici a velké písmeno,
    b) minimální doba platnosti hesla je 1 hodina,
    c) maximální platnost hesla je nastavena na 12 měsíců s vynucenou změnou (tj. nelze ji odložit),
    d) nelze použít 3 poslední zadaná hesla.
17. Operační systémy a aplikace organizace jsou nastaveny tak, aby neumožňovaly uživatelům měnit minimální požadavky na kvalitu hesla.
18. Správce ICT a administrátorské účty a pro přihlašování používají heslo splňující alespoň následující pravidla:
    a) minimální délka 15 znaků, obsahuje alespoň jednu číslici, malé a velké písmeno,
    b) minimální doba platnosti hesla je 1 den,
    c) maximální platnost hesla je nastavena na 12 měsíců s vynucenou změnou (tj. nelze ji odložit),
    d) nelze použít 5 posledních použitých hesel.
19. Přístup ke sdíleným složkám je zaměstnancům povolen pouze na základě zadání jejich uživatelského jména a hesla. Správce ICT definuje způsoby přístupu k těmto složkám a na základě schválení ředitele nastaví příslušná přístupová oprávnění jednotlivým uživatelům.

Článek 9
Fyzická bezpečnost

1. Organizace má definovaná režimová opatření pro provoz budov organizace.
2. Zaměstnanci, zacházející s písemnostmi, obsahujícími osobní údaje, mají dostatek uzamykatelných úložných prostor pro ukládání těchto dokumentů, která aktivně využívají.
3. Ředitel organizace stanovil klíčový režim (tzn. všechny klíče, přidělené zaměstnancům, jsou evidovány). Ředitel organizace nebo jím pověřená osoba je odpovědná za evidenci vydaných klíčů a za bezpečné uložení duplikátů klíčů v trezoru nebo uzamykatelné skříňce.
4. Úklid prostor organizace je prováděn vlastními zaměstnanci. Pokud jsou pro úklid využívány služby externího dodavatele, je úklid prostor, obsahující písemnosti s osobními údaji, prováděn za přítomnosti zaměstnanců organizace.
5. Servery a jiná klíčová síťová zařízení (např. NAS servery, routery apod.) jsou umístěny tak, aby bylo zabráněno nepovolaným osobám s těmito zařízeními jakkoliv manipulovat nebo je poškodit. Servery a jiná klíčová síťová zařízení jsou umístěny v uzamykatelných datových skříní. Tyto skříně jsou situovány v místnostech s řízeným vstupem osob.
6. Místnost, kde jsou zařízení umístěna, je opatřena dveřmi s bezpečnostním kováním a bezpečnostní vložkou třídy RC3 dle ČSN EN 1627. Přístup do těchto místností a do datových skříní mají pouze určení zaměstnanci.

Článek 10
Nakládání s osobními údaji

1. Data obsahující osobní údaje, která nejsou uložena v aplikaci (např. soubory MS Word, MS Excel apod.), ukládají zaměstnanci do určených adresářů na interní pevný disk

přidělené výpočetní techniky nebo dle požadavku ředitele organizace na síťové disky organizace.

2. Ukládání osobních údajů a jiných dat organizace do cloudových řešeních, které nejsou ve správě organizace, anebo není s poskytovatelem služby cloudového řešení podepsána zpracovatelská smlouva, je zakázáno.
3. Je dodržováno pravidlo „prázdného stolu", to znamená, že všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.
4. Zaměstnanci nekopírují, neukládají, nepřenáší osobní údaje a jiná data organizace mimo prostory organizace a obecně nepoužívají jakékoliv soukromé datové nosiče (např. CD, flash disky, externí HDD).
5. Soubory, obsahující osobní údaje, jsou primárně zasílány mimo organizaci prostřednictvím datové schránky. Pokud tak nelze učinit, musí zaměstnanec tento soubor uložit do souboru typu ZIP, RAR apod. zabezpečeného heslem, který je odeslán příjemci elektronickou poštou. Heslo je příjemci zasláno jiným komunikačním kanálem např. SMS. Pro zašifrování souboru je možné využít kvalifikovaný certifikát.
6. Soubory, obsahující zvláštní kategorie osobních údajů, jsou zasílány pouze prostřednictvím datové schránky.
7. Tisk dokumentů je prováděn na osobních tiskárnách umístěných v kanceláři zaměstnance nebo na společných tiskárnách, umístěných mimo místnost zaměstnance, pomocí zadání osobního kódu zaměstnance nebo přiložením identifikačního čipu k tiskárně.
8. Pro ukládání osobních údajů na přenosná paměťová zařízení (flash a externí pevné disky) nebo notebooky je vždy využito šifrování. Např. za pomoci softwaru BitLocker integrovaného do operačního systému Windows 10 ve verzi Professional a vyšší nebo jiného vhodného šifrovacího nástroje.
9. Organizace má nastavený automatizovaný systém zálohování důležitých částí počítačové sítě včetně síťových prostředků. Správce ICT dbá při nastavování automatizovaného zálohování na rizika spojená s možným znehodnocením záloh virovou nákazou, především ransomware.
10. Organizace v každý moment disponuje zálohami, které jsou off-line a nejsou starší 1 měsíce.
11. Pokud jsou média se zálohami přenášena mimo prostory organizace, je pro jejich ochranu využíváno šifrování.

Článek 11
Bezpečnost sítě

1. Pokud je Wi-Fi síť používána pro přístup k interní síti, a tedy i aplikacím organizace, je identita zaměstnance před zpřístupněním této sítě ověřena prostřednictvím zadání přístupových údajů. Bez ověření identity zaměstnance nejsou interní síť, aplikace nebo síťové disky zpřístupněny.
2. V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT. Heslo musí být jiné, než pro běžný učet Správce ICT.
3. Správce ICT provádí pravidelnou kontrolu funkčnosti a aktualizaci firmwaru routerů.
4. Přístup k zálohám a k síťovým prostředkům je striktně omezen jak na logické, tak i fyzické úrovni pouze na odpovědné osoby.

5. Pokud má správce ICT zřízen vzdálený přístup k routerům či jiným síťovým prvkům, je odpovědností správce ICT zabezpečit vzdálené připojení takovým způsobem, aby byla eliminována případná rizika útoku na síť právě přes tyto klíčové body sítě.
6. Správce ICT vede evidenci zaměstnanců a výpočetní techniky s povoleným vzdáleným přístupem. Tyto seznamy jsou v pravidelných intervalech (alespoň jedenkrát za rok) přezkoumávány ředitelem organizace, nebo jím pověřenou osobou.

Článek 12
Pravidla vzdáleného přístupu k síti organizace

1. Zaměstnanci organizace mají povoleno vykonávat pracovní činnost mimo objekty organizace.
2. Pravidla pro tento typ práce (tj. služební cesta nebo práce z domova tzv. Home Office) ze strany zaměstnanců jsou následující:
   a) Zaměstnanci mimo objekty organizace vykonávají pracovní úkoly ze zařízení (počítače a notebooky apod.) ve vlastnictví organizace.
   b) Zařízení jsou nastavena správcem ICT dle pravidel určených touto směrnicí.
   c) Všechny vzdálené přístupy k síti organizace povoluje ředitel.
   d) Zařízení, které je určeno pro vzdálený přístup k síti organizace či pro práci z domova je chráněno šifrováním, a to na úrovni celého disku.
   e) Zaměstnanec pro práci a připojení k internetu vždy využívá šifrovaného, zabezpečeného připojení pomocí VPN, či jiné obdobné, stejně bezpečné technologie.
   f) Zaměstnanec nenechává zařízení bez dozoru ve vypnutém nebo zapnutém stavu (např. v autě, čekárnách, restauracích, obchodě apod.).
   g) Zaměstnanec aktivně zabraňuje volnému odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, na lavičkách, v prostředcích hromadné dopravy apod.).
   h) Zařízení používá výhradně zaměstnanec, kterému byla takové zařízení svěřeno. Jakékoliv půjčování, přenechávání či jiné sdílení zařízení s jinými osobami je zakázáno (včetně rodinných příslušníků).
3. Pravidla pro tento typ práce (tj. služební cesta nebo práce z domova tzv. Home Office) ze strany správců ICT jsou následující:
   a) Všechna zařízení a uživatelé, kterým je umožněn vzdálený přístup k interní síti organizace, jsou zařazeny do zvláštní skupiny v rámci řízení přístupových účtů a zařízení (např. zvláštní skupina na firewallu apod.).
   b) Pokud zařízení není uvedeno ve zvláštní skupině pro vzdálený přístup, není mu umožněn vzdálený přístupu k interní síti organizace.
   c) Správce ICT odpovídá za jednotné a bezpečné nastavení všech zařízení organizace určených ke vzdálenému přístupu k síti nebo pro použití pro Home Office.
   d) Na zařízeních, u kterých je umožněn vzdálený přístup k síti organizace, je správci ICT nastaveno uzamykání uživatelského účtu při neaktivitě uživatele na maximálně 5 minut.
   e) Všichni uživatelé mají nastaveno automatické odpojení od VPN při neaktivitě delší než 30 min.

Článek 13
Pravidla použití mobilních zařízení

1. Mobilní zařízení (smartphony a tablety) používána pouze k běžné komunikaci a k připojení k pracovní e-mailové schránce jsou:
   a) Chráněna proti neoprávněnému přístupu heslem, pinem nebo otiskem prstu. Ochrana gestem je zakázána.
   b) Uzamčena maximálně po 5 minutách neaktivity uživatele.
   c) Vybavena antivirovou aplikací.

d) Alespoň 1x za měsíc aktualizována.

2. Zaměstnanci mohou přistupovat k aplikacím organizace obsahující osobní údaje z mobilních zařízení organizace stejně jako z mobilních zařízení, která nejsou v majetku organizace.

3. Mobilní zařízení v osobním vlastnictví i ve vlastnictví organizace používaná k přístupu k aplikacím obsahující osobní údaje musí splňovat tato pravidla:
   a) Mobilní zařízení jsou chráněna proti neoprávněnému přístupu heslem, pinem nebo otiskem prstu. Ochrana gestem je zakázána.
   b) Mobilní zařízení s vlastním operačním systémem jsou vybavena antivirovou aplikací.
   c) Mobilní zařízení má nastavené automatizované uzamykání při neaktivitě zaměstnance maximálně po dobu 5 minut.
   d) Zaměstnanci pro přístup k aplikacím využívají zřízené webové rozhraní či klientskou část aplikace.
   e) Zaměstnanci se k aplikacím organizace přihlašují za pomoci svého přihlašovacího jména a hesla.
   f) Přihlašovací jméno a heslo k aplikacím není v zařízeních ukládáno. Tzn. při každém použití aplikace je nezbytné se znovu přihlásit (zadat heslo).
   g) V případě ztráty či krádeže zařízení ve vlastnictví zaměstnance, které je využito k přístupu k aplikacím organizace, je nezbytné změnit přístupová hesla k používaným aplikacím a ihned kontaktovat pověřence pro ochranu osobních údajů.
   h) Je odpovědností zaměstnance nastavit své mobilní zařízení dle požadavků uvedených výše. v případě potřeby může kontaktovat správce ICT, který zaměstnanci s nastavením pomůže.
   i) Pokud mobilní zařízení není nastavené dle pravidle uvedených výše, je zakázáno jej používat pro připojení k jakýmkoliv aplikacím organizace.

Článek 14
Dodavatelé služeb ICT

1. Organizace identifikuje dodavatele aplikací a služeb ICT s možností přístupu k datům organizace (i vzdálený přístup např. pomocí VPN) a uzavře s nimi smlouvy, příp. dodatek smlouvy o zpracování osobních údajů v souladu s požadavky čl. 28 GDPR.

2. Správce ICT eviduje jednotlivé vzdálené přístupy dodavatelů a kontroluje jejich oprávněnost.

3. V rámci smluvního vztahu s dodavatelem si organizace stanoví předmět dodávané služby. V rámci klasifikace úrovně dodávky musí být minimálně stanoveny následující podmínky:
   a) stanovení předmětu a kvality služby,
   b) stanovení service level agreement SLA (pokud je předmětem dodávky služba),
   c) definice stížností, reklamací (stanovení postupů),
   d) eskalační procedura (v případě, že nelze s dodavatelem dohodnout řešení, mělo by být určeno, na kterou hierarchicky vyšší řídící úroveň se řešení problému přesune),
   e) nastavení kontrolních mechanismů v rámci předmětu dodávané služby,
   f) hodnocení a kontrola bezpečnostních opatření.

4. Za řízení dodavatelů je odpovědný ředitel organizace nebo jím pověřená osoba, která danou službu za organizaci zastřešuje.

5. O všech změnách, dohodách a kontrolách s dodavateli musí být proveden záznam.