Vnútorný predpis
číslo : 001 /2015

BEZPEČNOSTNÝ PROJEKT

informačného systému zameraný na ochranu osobných údajov obce Kysta

V Kyste, dňa 23.10.2015

.....
Mgr. Helena Borčíková
starostka obce

Článok 1
Úvodné ustanovenie

Starosta obce v Kyste v zmysle v súlade s § 19 ods. 3 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a § 5 vyhlášky č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení, vydáva týmto vnútorným predpisom Bezpečnostný projekt informačného systému obce Kysta . (ďalej len „Bezpečnostný projekt“).

Článok 2
Obsah „Bezpečnostného projektu“

Bezpečnostný projekt obce Kysta obsahuje :

1. Špecifikáciu informačného systému obce
2. Bezpečnostný zámer
3. Analýzu bezpečnosti informačného systému
4. Bezpečnostnú smernicu

Článok 3
Informačný systém obce

Obec Kysta je prevádzkovateľom informačného systému, ktorý pozostáva z dvoch samostatných pracovných staníc:

1. Pracovná stanica PCS01 v kancelárii starostu s pripojením na internet
   - prístup na www stránky a komunikácia cez internet
   - dokumentácia starostu

2. Pracovná stanica PCS02 v kancelárii obecného úradu
   - **program „ IFOSOFT“:** - evidencia obyvateľov
     - stály zoznam voličov
     - evidencia daňovníkov a poplatníkov
     - účtovníctvo
     - miestne dane a poplatky
     - majetok obce
     - personálna a mzdová agenda

Osoby zodpovedné za ochranu osobných údajov :

- Mgr. Helena Borčíková – starostka obce – štatutárny orgán
- Monika Pregová – zamestnanec obce poverený vedením evidencie obyvateľstva, stáleho zoznamu voličov, agendy miestnych daní, miestnych poplatkov, výkonom personálnej a mzdovej agendy, majetku obce, účtovníctva, evidencie hrobových miest

Článok 4
Bezpečnostný zámer

1. Základné bezpečnostné ciele

1. Zabezpečiť ochranu osobných údajov pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.
2. Minimalizovať riziká pri prevádzke informačného systému pred napadnutím aktív.
3. Zabezpečiť kontinuitu činností v informačnom systéme v prípade narušenia.
4. Zabezpečiť ochranu aktív.
5. Zabezpečiť ohodnotenie o ošetrenie rizík.
6. Zabezpečiť realizáciu preventívnych opatrení.
7. Zabezpečiť pripravenosť na aktívny prístup pri riešení akéhokoľvek narušenia.
8. Analyzovať možnosti napadnutia.
9. Stanoviť úrovne bezpečnosti.

2. Bezpečnostné opatrenia

Základnými bezpečnostnými opatreniami obce Kysta je súhrn:

· technických
· organizačných
· personálnych

opatrení, ktoré zabezpečujú ochranu osobných údajov v pôsobnosti obce.

A. Špecifikácia technických opatrení a spôsob ich využitia :

a/ Technické opatrenia predstavujú všetky určené technické prostriedky určené pre spracúvanie, manipuláciu, archiváciu a skartáciu osobných údajov a všetky prostriedky a metódy ochrany určených technických prostriedkov.

Používanie technických prostriedkov pre spracúvanie osobných údajov je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.

Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanca zodpovedného za výpočtovú techniku určí starosta obce.

b/ Technickými prostriedkami na účely zákona NR SR č. 122/2013 Z.z. sú :

1. Výpočtová technika - ktorou sa zabezpečuje vytváranie, spracovávanie, tlač a uchovávanie dát a informácii. Výpočtovú techniku tvorí komplex zariadení (technické a programové vybavenie, periférne zariadenia a podobne) a ich vzájomné prepojenie telekomunikačnými systémami a počítačovými sieťami a dátové nosiče (diskety, pásky, CD disky a pod.)

2. Zariadenie na vyhotovenie písaného textu - tlačiarne pri osobných počítačoch a severoch, rozmnožovacie stroje.

3. Zabezpečenie uvedených technických prostriedkov je vykonávané programovými, mechanickými, režimovými a technickými prostriedkami ochrany.

- **programová ochrana** - antivírové programy, vstupné a prihlasovacie heslá, používanie iba autorizovaných programov,
- **mechanická ochrana** - vybavenie určených pracovísk mrežami, plnými dverami, zaslepenými kľučkami,
- **režimová ochrana** - určenie režimu vstupu na pracoviská, zákaz zdržovania sa po pracovnej dobe, určenie zodpovedných zamestnancov za bezpečnosť, určeniepodmienok vstupu na pracovisko a spôsob opustenia pracoviska a pod.
- **technická ochrana** – požiarno-bezpečnostné opatrenia, požiarna signalizácia, signalizácia neoprávneného vstupu a pod.

B. Špecifikácia organizačných opatrení a spôsob ich využitia

a/ Organizačné opatrenia predstavujú zákonné normy, predpisy a nariadenia, podľa ktorých sa riadi činnosť určených pracovísk pre spracúvanie, ukladanie, manipuláciu, archiváciu a skartáciu osobných údajov.

b/ Požiadavky na organizačné opatrenia.

Zabezpečenie bezpečnostných opatrení pri ochrane osobných údajov pomocou organizačných opatrení, ktorými sú organizované pracovné činnosti a postupy pri zabezpečovaní celkovej, informačnej a počítačovej bezpečnosti.

Organizačné opatrenie obsahujú:

- Definovanie organizačnej štruktúry
- Rozdelenie kompetencií
- Určenie pracovných a bezpečnostných postupov
- Organizačné opatrenia

Základnú normu tvorí štatút obce a organizačný poriadok obecného úradu obce Kysta. Starosta obce menuje krízový štáb (havarijný tím), ktorý zabezpečí kontinuitu činností v prípade narušenia informačného systému, mimoriadnej udalosti, živelnej pohromy a inej nepredvídanej situácie.

Pre krízový štáb musí byť zrejmé:

- Personálne obsadenie
- Spôsob komunikácie
- Prerozdelenie úloh medzi členmi tímov
- Krízový štáb má právomoci vydávať rozhodnutia

C. Špecifikácia personálnych opatrení a spôsob ich využitia

a/ Personálne opatrenia - personálna bezpečnosť- je zákonom stanovený postup (§ 21 a § 22 zákona NR SR č. 122/2013 Z. z.), ktorý určuje predpoklady k získaniu oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti oprávnených osôb. Personálna bezpečnosť zahŕňa vedenie predpísanej evidencie, na ochranu osobných údajov.

Starostka obce Kysta, Mgr. Helena Borčíková písomne poverí výkonom dohľadu nad ochranou osobných údajov spracúvaných podľa zákona NR SR č. 122/2013 Z. z. zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

b/ Pri spracovávaní osobných údajov v informačnom systéme sú oprávnené osoby povinné dodržiavať príkaz starostky obce Kysta o pravidlách používania lokálnej počítačovej siete.

c/ Požiadavky na personálne opatrenia

- Stanoviť kvalifikačné predpoklady
- Personálne zabezpečiť všetky procesy
- Definovať personálnu bezpečnosť
- Zabezpečiť zastupiteľnosť
- Zabezpečiť dodržiavanie bezpečnostných smerníc
- Zabezpečiť školenia k bezpečnostným smerniciam a novým právnym predpisom

3. Okolie informačného systému a jeho vzťah k možnému narušeniu bezpečnosti

Obec Kysta prevádzkuje informačný systém v dvoch samostatných personálnych počítačoch PCS01 a PCS02. PCS01 je pripojený do siete internet pevným pripojením. Pripojenie k internetu je využívané na prístup k www stránkam a na komunikáciu.

Prostriedky zabezpečenia informačného systému slúžia na minimalizáciu rizík.

Osobné údaje sú spracovávané na pracoviskách obce Kysta so stálou službou ochrany počas pracovnej doby. Nie je možné vylúčiť priame napadnutie pracoviska mimo pracovných hodín.

5. Vymedzenie hraníc určujúcich množinu zvyškových rizík

Hranicu zvyškových rizík stanovuje súbor všetkých opatrení pomocou ktorých je zabezpečený normálny chod informačného systému /IS/ a sú splnené všetky podmienky na dodržanie zásad ochrany IS. Množina zvyškových rizík je ohraničená nepredvídateľnými udalosťami alebo činnosťami, ktoré sa nedajú ovplyvniť. Zvyškové riziká môžu mať za následok čiastočne narušenie IS, alebo úplné narušenie aktív s znefunkčnením informačného systému.

Definovanie množiny zvyškových rizík.

Vplyv na znefunkčnenie IS	Riziká	Hrozba
Čiastočné	Napadnutie hrubou silou	· Vyradenie bezpečnostného systému · Prelomenie technických zábran vstupov : mreží, bezpečnostných dverí · Krádež dokumentov · Krádež technických prostriedkov informačného systému · Znefunkčnenie technických prostriedkov
Čiastočné	Narušenie aktív následkom porúch technologických zariadení	· Porucha na vodovodnom, kanalizačnom a vykurovacom potrubí
Úplné	Živelná pohroma	· Povodeň · Zasiahnutie bleskom - požiar · Zemetrasenie
Úplné	Teroristický útok	· Výbuch · Zamorenie · Požiar
Úplné	Porucha na technologickom zariadení	· Zamorenie priestoru · Požiar

Článok 5
Analýza bezpečnosti informačného systému

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému.

1. Identifikácia a analýza rizík

a/ Neoprávnená modifikácia osobných údajov

Dopad hrozby na aktíva systému: narušenie integrity, dostupnosti, dôvernosti.
Potencionálne slabiny: zmeny programov, vrátane zavedenia škodlivých programov (rôznych červov, logických bômb, trójskych koni, zadných vrátok atd'.), zmeny súborov s citlivými údajmi.

Súčasný stav zabezpečenia:
- je nainštalovaná antivírová ochrana
- pracovná stanica PCS02 nie je pripojená do žiadnej počítačovej siete
- je potrebné prenášať údaje na prenosných médiách medzi PCS 01 a PCS02

b/ Neoprávnený lokálny prístup k osobným údajom v pracovnej stanici

Dopad hrozby na aktíva systému: narušenie integrity a dôvernosti.
Potencionálne slabiny: neoprávnená osoba môže získať neautorizovaný prístup k údajom vplyvom nepoužívania hardvérových alebo softvérových autentizačných prostriedkov, krátkodobé opustenie počítača, čítanie údajov z obrazovky monitora neoprávnenou osobou.

c/ Minimalizácia rizík

- kontrola používania PC z hľadiska zabezpečenia antivírovou ochranou,
- kontrola používaných prenosných médií,
- zabezpečenie PC pred nepovolanými osobami,

2. Bezpečnostné štandardy, metódy a prostriedky ochrany osobných údajov v informačnom systéme

Súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami.

1. Ochrana osobných údajov sa rieši v súlade so zákonom NR SR č. 122/2013 Z. z. o ochrane osobných údajov. Ďalej vychádza z nasledujúcich zákonov:

· Zákon NR SR č. 215/2002 Z. z. o elektronickom podpise

· Zákon NR SR č. 261/1995 Z. z. o štátnom informačnom systéme

· Zákon NR SR č. 211/2000 Z. z. o slobodnom prístupe k informáciám

· Pre metodiku sa použijú aj :

· Zákon NR SR č. 241/2001 Z. z. o ochrane utajovaných skutočností

· Vyhláška NBÚ č. 455/2001 Z. z. o administratívnej bezpečnosti

· Vyhláška NBÚ č. 2/2002 Z. z. o personálnej bezpečnosti

· Vyhláška NBÚ č. 28/2002 Z. z. o priemyselnej bezpečnosti

· Vyhláška NBÚ č. 88/2002 Z. z. o fyzickej a objektovej bezpečnosti

· Vyhláška NBÚ č. 90/2002 Z. z. o bezpečnosti technických prostriedkov

· Vyhláška NBÚ č. 537/2002 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky)

· Vyhláška NBÚ č. 542/2002 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku

3. Zabezpečenie Informačného systému pred hrozbami :

Hrozby	Úroveň bezpečnosti	Opatrenia
1. Prírodné udalosti	Globálna	Technické
a. Búrka, blesk	Zvyškové riziko	Zabezpečené polohou
b. Potopa	Globálna	Technické
c. Námraza	Zvyškové riziko	Havarijný plán
d. Zemetrasenie		
2. Technologické havárie	Globálna	Technické
a. Požiar	Zvyškové riziko	Havarijný plán
b. Únik nebezpečných látok	Zvyškové riziko	Havarijný plán
c. Únik nebezpečných látok mimo objekt	Zvyškové riziko	Havarijný plán
d. Výbuch		

3. Sociálne a. Štrajk, nespokojnosť zamestnancov b. Politické zámery	Globálna Globálna	Organizačné, personálne Organizačné
4. Organizačné a. Nepokryté pracovné postupy b. Kompetenčné	Globálna Globálna	Organizačné Personálne, organizačné
5. Výpadky a. Technologické b. Infraštruktúry c. Komunikačné linky d. Server e. Služby	Globálna Globálna, informačná Informačná Počítačová Globálna, informačná, počítačová	Technické Organizačné Technické Technické Organizačné, personálne
6. Infiltrácia a. Ľudské – vnútorné b. Ľudské – vonkajšie c. Počítačová	Globálna Počítačová, informačná	Personálne, organizačné Technické, organizačné
7. Chyby a. HW b. SW c. Užívateľov d. Správcov	Počítačová, informačná Počítačová Globálna Globálna	Technické Technické Personálne, organizačné Personálne

Článok 6
Bezpečnostná smernica

Bezpečnostná smernica je tvorená bezpečnostnými opatreniami, ktoré sú samostatnými smernicami v oblastiach upravovaných zákonom č. 122/2013 Zz. o ochrane osobných údajov a vyhláškou č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení.

Zoznam smerníc :

1. Smernica o ochrane osobných údajov a o podpore bezpečnosti IS pre vedúcich zamestnancov obce,
2. Smernica o ochrane osobných údajov a o zásadách bezpečnosti pre používateľov IS obce,

3. Smernica o ochrane osobných údajov a o zásadách bezpečnosti pri prevádzke informačných a komunikačných technológií IS obce,
4. Havarijný plán IS obce

1. Smernica o ochrane osobných údajov a o podpore bezpečnosti IS pre vedúcich zamestnancov obce Kysta

Článok 1
Všeobecné ustanovenia

1. Táto smernica upravuje základné zásady pre vedúceho zamestnanca obce Kysta pre podporu bezpečnej a spoľahlivej prevádzky informačného systému obecného úradu (ďalej len "IS").
2. Vedúcim zamestnancom organizačného útvaru IS je : starosta obce.

Článok 2
Ochrana osobných údajov

1. Vedúci zamestnanec je povinný dbať o to, aby sa v jeho útvare spracúvali osobné údaje len v nevyhnutne potrebnom rozsahu a na nevyhnutne potrebnú dobu. Taktiež je povinný dbať o náležitú ochranu osobných údajov spracúvaných v útvare, t.j. obmedzenie prístupu k zhromaždeným a spracúvaným osobným údajom len na zamestnancov, ktorí prístup k týmto údajom potrebujú na plnenie svojich pracovných úloh.
2. Vedúci zamestnanec je povinný zabezpečiť náležité poučenie osôb, ktoré môžu prísť do styku s osobnými údajmi spracúvanými v podmienkach obce resp. obcou zriadeného organizačného útvaru, o povinnostiach ochrany osobných údajov a o povinnosti mlčanlivosti o osobných údajoch, s ktorými prišli do styku.
3. Vedúci zamestnanec je povinný organizovať prácu podriadeného zamestnanca povereného spracovávaním osobných údajov tak, aby sa osobné údaje v listinnej forme spracúvali a skladovali iba vo vyhradených priestoroch pracoviska a s využitím dostupných prostriedkov ich zabezpečenia (uzamykanie priestorov, skladovanie v uzamykateľných skrinkách, a pod.). Taktiež je povinný organizovať prácu podriadeného zamestnanca pri vzniku či riešení mimoriadnej situácie tak, aby boli zachované základné bezpečnostné zásady pre prístup k osobným údajom, t.j. predovšetkým obmedzenie prístupu neoprávnených osôb k osobným údajom spracúvaným v podriadenom útvare.
4. Vedúci zamestnanec je povinný spolupracovať s osobou poverenou výkonom dohľadu nad ochranou osobných údajov na pracovisku, konzultovať s ňou otázky prípadnej zmeny rozsahu, účelu a spôsobu spracovania osobných údajov spracúvaných a skladovaných v podriadenom útvare, ako aj dbať o aktuálnosť údajov príslušnej časť evidencie

informačných systémov, vedenej v zmysle požiadaviek § 28 a 29 zákona č. 428/2002 Z.z. o ochrane osobných údajov.

Článok 3
Základné zásady pre podporu bezpečnosti IS

1. Vedúci zamestnanec pridelí prístupové práva do IS pre podriadených zamestnancov tak, aby sa rešpektoval bezpečnostný princíp "najmenších privilégií" (zamestnanec má mať pridelené len také privilégia, ktoré potrebuje pre plnenie svojich pracovných povinností, a nie vyššie).
2. Vedúci zamestnanec je zodpovedný za uloženie zalepených obálok vstupných hesiel do aplikačného programového vybavenia podriadených zamestnancov pre prípad núdzového použitia týchto aplikácií.
3. Vedúci zamestnanec je zodpovedný za včasné zrušenie, príp. modifikáciu prístupových práv podriadeného zamestnanca, ktorému končí pracovný pomer, resp. ktorému sa zásadným spôsobom zmenila pracovná náplň. Vedúci zamestnanec je povinný rozhodnúť o súboroch podriadeného zamestnanca, ktorému sa končí pracovný pomer – prideliť ich inému zamestnancovi, rozhodnúť o ich archivovaní, alebo rozhodnúť o ich odstránení ku dňu ukončenia pracovného pomeru zamestnanca, ktorý s nimi dovtedy pracoval.
4. Vedúci zamestnanec je povinný riešiť zastupovanie neprítomného podriadeného zamestnanca – používateľa IS zamestnancom, ktorý má pridelené obdobné prístupové práva ako zastupovaná osoba, alebo určiť dočasné rozšírenie prístupových práv zastupujúcej osoby na určenú dobu.
5. Vedúci zamestnanec je povinný vlastným rešpektovaním bezpečnostných zásad pri používaní IS, ako aj bezodkladným riešením zistených nedostatkov v dodržiavaní bezpečnostných zásad podriadenými zamestnancami usilovať sa o zaradenie bezpečnostných zásad a postupov do návykov spojených s rutinnou prácou podriadených zamestnancov - používateľov IS.
6. Vedúci zamestnanec je povinný pri vydávaní pokynov podriadeným zamestnancom striktne rešpektovať ustanovenia platných smerníc o bezpečnosti IS a nevydávať príkazy, ktoré sú v konflikte so zásadami uvedenými v týchto smerniciach.
7. Vedúci zamestnanec je povinný dbať o trvalú primeranú úroveň vedomostí a skúseností podriadených zamestnancov - používateľov IS, potrebnú pre bezpečnú a spoľahlivú prácu so systémom. Za týmto účelom je povinný umožniť podriadeným zamestnancom primerané vzdelávanie zamerané na prácu s IS a na zásady bezpečnosti pri práci s týmto systémom.
8. Vedúci zamestnanec je povinný v prípade výrazných zmien v zameraní práce útvaru, resp. v práci podriadených zamestnancov prehodnotiť adekvátnosť prístupových práv pridelených podriadeným zamestnancom (obzvlášť rešpektovanie princípu najmenších privilégií).
9. Vedúci zamestnanec je povinný bezodkladne riešiť a v prípade potreby rozhodnúť o všetkých podnetoch podriadených zamestnancov, ako aj vlastné zistenia týkajúce sa:

a) podozrenia z narušenia bezpečnosti IS,
b) nedostatkov v návrhu alebo prevádzke IS, ktoré by mohli mať za následok zníženie úrovne bezpečnosti IS,
c) návrhov na zlepšenie systému zabezpečenia IS.

Článok 4
Záverečné ustanovenia

1. Porušenie tejto smernice bude posudzované ako závažné porušenie pracovnej disciplíny zamestnanca v zmysle príslušných ustanovení Zákonníka práce resp. zákona č. 552/2003 Z.z. o výkone prác vo verejnom záujme v znení neskorších predpisov
2. Táto smernica nadobúda účinnosť dňom 10.01.2015.

2. Smernica o ochrane osobných údajov a o zásadách bezpečnosti pre používateľov informačného systému obce Kysta

Článok 1
Všeobecné ustanovenia

Táto smernica upravuje základné pravidlá pre ochranu osobných údajov v elektronickej a listinnej forme a pre zaistenie bezpečnej a spoľahlivej prevádzky pracovných staníc a informačného systému obce Kysta (ďalej len "IS").

Používateľmi IS (ďalej len "používatelia") sú zamestnanci obce Kysta (obecného úradu).

Článok 2
Ochrana osobných údajov

1. Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, teda údaje, z ktorých možno identifikovať osobu, ktorej sa týkajú.
2. Pod ochranou osobných údajov sa rozumie splnenie požiadaviek, ktoré stanovuje zákon č. 428/2002 Z.z. o ochrane osobných údajov, predovšetkým
   - účelnosť zhromažďovania a spracúvania osobných údajov (zhromažďuje a spracúva sa len nevyhnutne potrebný rozsah osobných údajov a len na nevyhnutne potrebnú dobu)
   - obmedzenie prístupu k zhromaždeným a spracúvaným osobným údajom len na zamestnancov, ktorí prístup k týmto údajom potrebujú na plnenie svojich pracovných úloh
3. Zhromažďovať a spracúvať osobné údaje spolu s rodným číslom dotknutých osôb je prípustné len na účely obvyklých agend príslušných útvarov pracoviska. Nie je povolené zhromažďovanie a spracúvanie osobných údajov nad rámec agend uložených pracovisku príslušnými právnymi predpismi.
4. V zásade, prístup k spracúvaným osobným údajom môžu mať len pracovníci zodpovední za príslušnú agendu. Externý dodávateľ služieb, ktorého zamestnanci pri výkone dohodnutých služieb môžu prísť do styku s osobnými údajmi spracúvanými na pracovisku, sa k povinnosti ochrany osobných údajov spoločnosti a k záväzku mlčanlivosti zaviaže podpisom zmluvy, ktorou sa utvára zmluvný vzťah s pracoviskom, a ktorá musí obsahovať ustanovenie o tomto záväzku.
5. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností môžu prísť do styku s osobnými údajmi spracúvanými na pracovisku, sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku. Povinnosť mlčanlivosti trvá aj po zániku ich funkcie alebo pracovného pomeru.

6. Osobné údaje sa môžu zhromažďovať a spracúvať len v priestoroch príslušného útvaru pracoviska /obecného úradu, resp. pracoviska MŠ a inej organizácie zriadenej obcou/.Výnimky z tohto pravidla môžu byť udelené len na nevyhnutne potrebnú dobu pri rešpektovaní požiadaviek na zaistenie náležitej ochrany spracúvaných osobných údajov. O udelení výnimky rozhoduje starosta obce, resp. príslušný štatutárny zástupca. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností zhromažďujú alebo spracúvajú osobné údaje, sú povinní ohlásiť príslušnému vedúcemu zamestnancovi v rámci pracoviska, každý zistený prípad či vážne podozrenie na únik osobných údajov, neoprávnené zasahovanie do osobných údajov, či zistenie o nedostatočnej účinnosti existujúcich bezpečnostných opatrení prijatých na ochranu osobných údajov.
7. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností zhromažďujú alebo spracúvajú osobné údaje v listinnej forme, sú povinní využiť všetky dostupné prostriedky pre zabezpečenie týchto údajov pred prístupom neoprávnených osôb – skladovanie údajov v uzamknutých častiach nábytku, uzamykanie kancelárii, alebo aspoň zabezpečenia náležitého dozoru príslušných priestorov počas svojej neprítomnosti, ako aj ochrana príslušných kľúčov pred ich získaním neoprávnenými osobami. Taktiež sú povinní, pokiaľ iné predpisy neprikazujú inak, bez zbytočného odkladu spoľahlivým spôsobom zlikvidovať nepotrebné, alebo chybné dokumenty obsahujúce osobné údaje.
8. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností zhromažďujú alebo spracúvajú osobné údaje v elektronickej forme, sú povinní využiť všetky dostupné prostriedky, ktoré pre kontrolu prístupu k spracúvaným údajom ponúka príslušné programové vybavenie, teda predovšetkým prístupové heslá. Taktiež sú povinní počas svojej neprítomnosti ponechať príslušnú pracovnú stanicu v stave, v ktorom je prístup k osobným údajom viazaný na znalosť príslušného prístupového hesla (pracovná stanica odhlásená zo systému, či aspoň chránená šetričom obrazovky s heslom).
9. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností zhromažďujú alebo spracúvajú osobné údaje v elektronickej forme, sú povinní v prípade tlače výstupov obsahujúcich osobné údaje zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce osobné údaje musia byť skladované, resp. zlikvidované tak, aby nedošlo k narušeniu ich dôvernosti.
10. Zamestnanci, ktorí v rámci výkonu svojich pracovných povinností zhromažďujú alebo spracúvajú osobné údaje, zodpovedajú za to, že v priebehu mimoriadnej situácie, ako aj riešení jej následkov (obnova pôvodného stavu) budú zachované základné bezpečnostné zásady pre prístup k osobným údajom v ich oblasti pôsobnosti. Cieľom je aj v priebehu mimoriadnej situácie, resp. pri riešení jej následkov obmedziť prístup neoprávnených osôb k osobným údajom spracúvaným na pracovisku.
11. V prípade, že v priebehu mimoriadnej situácie, resp. riešení jej následkov, nebude možné dosiahnuť cieľ stanovený v predchádzajúcom bode, cieľom bude dosiahnuť, aby doba zníženej ochrany osobných údajov bola čo najkratšia a aby sa zdokumentoval stav a manipulácia so zariadeniami, resp. médiami obsahujúcimi osobné údaje počas doby zníženej ochrany. Predovšetkým ide o zdokumentovanie kde boli osobné údaje (dočasne) umiestnené, na akú dlhú dobu, či a ako boli zabezpečené a ktoré neoprávnené osoby mali k nim prístup. Tieto informácie sa bez zbytočného odkladu poskytnú osobe poverenej výkonom dohľadu nad ochranou osobných údajov.

Článok 3
Manipulácia s technickými prostriedkami IS

1. Pracovné stanice IS musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.). Pracovné stanice neumiestňovať na podlahu a v jej blízkosti.
2. Používateľ môže manipulovať s pracovnými stanicami IS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
3. Používateľ nesmie znižovať životnosť pracovných staníc IS hrubým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení IS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení), resp. znížením ich životnosti alebo spoľahlivosti (vibrácie a pod.).
5. Používateľ nemôže:
   a) robiť zásahy do pracovných staníc IS,
   b) pripájať k pracovným staniciam ďalšie technické zariadenia,
   c) odpájať technické zariadenia pracovnej stanice,
   d) premiestňovať pracovné stanice,
   e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a reštartovanie počítača a tlačiarne, vkladanie a vyberanie diskiet a CD z mechaník, výmena tonera, ovládanie nastavenia jasu, kontrastu, príp. ďalších prvkov regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.
6. Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom starostu obce. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
7. Čistenie povrchu technických zariadení pracovnej stanice od prachu je povinný vykonávať používateľ pracovnej stanice vhodnými čistiacimi prostriedkami pri vypnutom stave zariadenia. Vnútorné čistenie zariadení IS môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.
8. Odnímateľné pamäťové médiá používané na ukladanie údajov (diskety, CD, USB pamäťové moduly a podobne) musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne) tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované teplotným extrémom, vlhkosti a prašnosti.
9. Do mechaník prenosných pamäťových médií (diskiet, pások, CD) nesmú byť vkladané znečistené alebo poškodené médiá.
10. Pri zapínaní a reštartovaní počítača nesmie byť v disketovej alebo CD mechanike založené pamäťové médium.

Článok 4
Základné zásady pre manipuláciu s programovým vybavením IS

1. Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom starostu. Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
2. Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
3. Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.
4. Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.
5. Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
6. Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice - okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).
7. Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť starostovi obce.

Článok 5
Prístupové heslá

1. Používateľ je povinný svoje prístupové heslá meniť najmenej jeden krát za 6 mesiacov, príp. aj na pokyn starostu obce.
2. Prístupové heslá používateľa musia mať aspoň 5 znakov (prístupové heslo šetriča obrazovky aspoň 4 znaky). Používateľ nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napr. meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a pod.
3. Používateľ musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba (vrátane iných používateľov). Používateľ si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom.

4. V prípade podozrenia, že iná osoba pozná heslo používateľa je používateľ povinný príslušné heslo okamžite zmeniť a svoje podozrenie ohlásiť starostovi obce.
5. Používateľ sa prihlasuje do siete a do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému používateľovi.
6. Používateľ je povinný pre núdzové prípady svoje heslo do aplikácie uložiť v zalepenej obálke u vedúceho príslušného organizačného útvaru.

Článok 6
Manipulácia s údajmi IS

1. Za zálohovanie údajov na lokálnom disku pracovnej stanice, v prípade, že ich používateľ vytvára a používa pri svojej práci, je zodpovedný používateľ. Používateľ je v takom prípade zodpovedný aj za bezpečné uskladnenie pamäťových médií obsahujúcich záložné kópie údajov.
2. Používateľ môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi. Výnimku tvoria údaje už zverejnené alebo určené na zverejnenie.

Článok 7
Antivírusové opatrenia

1. Je zakázaný akýkoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej stanice používateľom.
2. Používateľ je povinný pred použitím nosičov dát (diskety, CD) otestovať ich na prípadný výskyt vírusov.
3. Používateľ je povinný mesačne alebo v prípade podozrenia na výskyt vírusu otestovať pracovnú stanicu.
4. V prípade, že sa na pracovnej ploche používateľa zobrazí varovanie, že sa na disku, vloženej diskete alebo CD nachádza vírus, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírená disketa alebo CD patrí inému subjektu, používateľ ju viditeľne a výrazne označí ako zavírenú a vráti ju jej majiteľovi. V prípade zavírenia pevného disku, vlastnej diskety alebo CD používateľ túto skutočnosť bezodkladne oznámi informatikovi a disketu alebo CD viditeľne a výrazne označí ako zavírenú. V prípade zavírenia CD-R, používateľ je povinný médium viditeľne označiť ako zavírené a vyradiť z používania.
5. V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí starostu obce, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi.
6. Je zakázané otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa (používateľ je povinný hodnovernosť obsahu správy overiť u odosielateľa) .

Článok 8
Zaznamenávanie a hlásenie problémov s pracovnou stanicou

1. Používateľ pracovnej stanice zaznamená a zodpovednému vedúcemu bezodkladne ohlási každú vnímateľnú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým však nasledovné udalosti:

a) hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo,

b) problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov a viditeľných javov, ktoré predchádzali, resp. nasledovali výskyt problému).

2. Používateľ pracovnej stanice zaznamená a svojmu nadriadenému bezodkladne ohlási každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti IS, predovšetkým však nasledovné udalosti:
    a) výskyt vírusu (prepis varovného hlásenia),
    b) únik údajov, s informáciou, aké informácie unikli, kam a ako,
    c) odcudzenie médií s údajmi z pracovnej stanice,
    d) odcudzenie technických zariadení pracovnej stanice,
    e) neoprávnený zásah do technických zariadení pracovnej stanice,
    f) neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice).
3. Vyššie uvedené zásady platia aj v prípade, že používateľ dočasne používa pracovnú stanicu pridelenú inému používateľovi; v takom prípade navyše informuje aj používateľa, ktorému bola pracovná stanica pridelená.
4. Používateľ informuje svojho nadriadeného aj v prípade, keď má podozrenie, že súčasný stav umožňuje narušenie bezpečnosti alebo funkčnosti IS.
5. Používatelia sú povinní spolupracovať pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré by zabránili výskytu podobnej situácie.

Článok 9
Využívanie sieťových služieb (Internet)

1. Každý používateľ, ktorému bol umožnený prístup do siete Internet, je povinný rešpektovať nasledovné zásady:
    a) prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou a činnosťou príslušného organizačného útvaru,

b) svojou činnosťou v sieti Internet reprezentuje nielen seba ale aj úrad, ktorý mu prístup do siete umožnilo. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena úradu alebo k iným škodám,

c) komunikácia v Internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,

d) elektronická pošta sa dá sfalšovať. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mal používateľ realizovať závažné kroky, je povinný si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ,

e) Internet je bohatým zdrojom nielen informácií, ale aj rôznych programov. Pre získavanie programového vybavenia a jeho použitie na počítačových systémoch pracoviska platia rovnaké pravidlá, ako pre ostatné programové vybavenie (pozri článok 4).

Článok 10
Záverečné ustanovenia

1. V prípade bezpečnostného incidentu používateľovi bude dočasne odobraté prístupové právo do IS do doby objasnenia. Používateľ je povinný za účelom objasnenia poskytnúť starostovi obce všetky potrebné informácie a technické prostriedky, ktoré s incidentom súvisia.
2. Porušenie tejto smernice bude posudzované ako závažné porušenie pracovnej a služobnej disciplíny zamestnanca v zmysle príslušných ustanovení Zákonníka práce resp. zákona č. 552/2003 Z.z. o o výkone prác vo verejnom záujme.
3. Táto smernica nadobúda účinnosť dňom 10.01.2015.

3. Smernica o ochrane osobných údajov o zásadách bezpečnosti pri prevádzke informačných a komunikačných technológií informačného systému obce Kysta

Článok 1
Všeobecné ustanovenia

1. Táto smernica upravuje základné pravidlá pre ochranu osobných údajov v elektronickej forme a pre zaistenie bezpečnej a spoľahlivej prevádzky informačných a komunikačných technológií informačného systému obce Kysta (ďalej len "IS").
2. Prevádzku informačných a komunikačných technológií IS zabezpečujú starosta obce a poverený zamestnanec /ďalej len „zodpovedné osoby"/.

Článok 2
Ochrana osobných údajov

1. Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, teda údaje, z ktorých možno identifikovať osobu, ktorej sa týkajú. Starosta obce a poverený zamestnanec pri plnení svojich pracovných úloh prichádzajú do styku s osobnými údajmi v elektronickej forme spracúvanými v podmienkach obce a sú teda povinní zabezpečiť náležitú ochranu spracúvaných osobných údajov.
2. Pod ochranou osobných údajov sa rozumie splnenie požiadaviek, ktoré stanovuje zákon č. 428/2002 Z.z. o ochrane osobných údajov, predovšetkým obmedzenie prístupu k zhromaždeným a spracúvaným osobným údajom len na osoby, ktoré prístup k týmto údajom potrebujú na plnenie svojich pracovných úloh.
3. Zodpovedné osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku. Povinnosť mlčanlivosti trvá aj po zániku ich funkcie alebo pracovného pomeru.
4. Zodpovedné osoby sú zodpovedné za také nastavenie prostriedkov informačných a komunikačných technológií, používaných na spracúvanie, ukladanie, alebo prenos osobných údajov v elektronickej forme ktoré zabezpečí, aby prístup k osobným údajom bol podmienený úspešnou identifikáciou a autentifikáciou oprávneného používateľa IS (zadanie správnej kombinácie mena a prístupového hesla oprávneného používateľa). Taktiež umožnia používateľom využívať na pracovných staniciach používaných pre prácu s osobnými údajmi šetrič obrazovky s heslom na ochranu prístupu do pracovnej stanice prihlásenej do systému počas krátkodobej neprítomnosti používateľa..
5. Prístupové práva pre prácu osobnými údajmi musia byť nastavené v súlade s bezpečnostným "princípom najmenších privilégií". Za prideľovanie a prípadnú zmenu prístupových práv používateľom podľa tohto princípu zodpovedá správca systému. Za včasné informovanie správcu systému o zmenách s dopadom na prístupové práva zamestnanca (preradenie na inú

prácu, rozviazania pracovného pomeru a pod.) zodpovedá vedúci zamestnanec útvaru, v ktorom používateľ pôsobí.

6. V záujme zabránenia prístupu neoprávnených osôb k starším kópiám osobných údajov zabezpečia zodpovedné osoby spoľahlivú likvidáciu (vymazanie) údajov zo všetkých pamäťových médií, ktoré obsahovali osobné údaje a ktoré sa vyraďujú, resp. preraďujú na iné využitie ako na spracovanie (uloženie) osobných údajov. V prípade samostatných médií u ktorých sa nepredpokladá opakované použitie, zabezpečia spoľahlivú likvidáciu médií spolu s údajmi na nich uloženými.

Článok 3
Kľúčové komponenty IS

1. Pre účely tejto smernice kľúčové komponenty IS sú tie technické a programové prostriedky a dokumenty, ktorých poškodenie, zlyhanie, alebo neoprávnená manipulácia nimi môže mať za následok ohrozenie spoľahlivej a bezpečnej prevádzky IS. Medzi kľúčové komponenty IS obce a patria pracovné stanice PCS01 v kancelárii starostu a PCS02 v kancelárii obecného úradu, záložný zdroj (ďalej len "UPS") týchto pracovných staníc, router pre pripojenie PCS01 k internetu, systémové a aplikačné programové vybavenie používané v rámci IS, pamäťové média obsahujúce záložné kópie údajov IS, inštalačné média pre základné a aplikačné programové vybavenie IS, zoznam prístupových hesiel pre použitie v prípade neprítomnosti správcu systému a pod.
2. Prístup ku kľúčovým komponentom IS majú len zodpovedné osoby.
3. Pre vstup do priestorov, kde sú uložené kľúčové komponenty IS je potrebné dodržiavať kľúčový režim.
4. Upratovanie a podobné práce v miestnostiach kde sú uložené kľúčové komponenty IS sa vykonávajú v prítomnosti zodpovednej osoby. Osoby vykonávajúce zmienené práce musia byť vopred riadne poučené o zákaze akokoľvek manipulovať s elektronickými zariadeniami bez predchádzajúceho súhlasu informatika.

Článok 4
Základné zásady bezpečnej prevádzky IS

1. Opravy, úpravy a akýkoľvek zásah na všetkých komponentov IS môžu vykonávať len kvalifikované osoby, konajúce na základe platného, vopred daného poverenia, resp. súhlasu Informatika. Všetky opravy a úpravy musia byť primerane zdokumentované.
2. Pri odstraňovaní porúch kľúčových komponentov IS je zodpovedné osoby oprávnené vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre odstránenie poruchy.
3. Na počítačoch IS je zakázané inštalovať a prevádzkovať programové vybavenie získané nelegálnym spôsobom, resp. porušujúce platné licenčné podmienky.

4. Starosta obce je povinný zabezpečiť antivírovú ochranu IS pracoviska kvalitným antivírovým prostriedkom a zabezpečiť jeho včasnú aktualizáciu.
5. V prípade vyraďovania počítačových systémov a médií sú zodpovedné osoby povinné zabezpečiť dôkladnú likvidáciu údajov IS na vyraďovaných zariadeniach a médiách.
6. Každá zodpovedná osoby je povinná pri dlhodobom opustení miestnosti, v ktorej je uložená jemu pridelená pracovná stanica, odhlásiť sa zo systému. V prípade krátkodobého opustenia miestnosti musí aspoň aktivovať šetrič obrazovky s heslom.

Článok 5
Zálohovanie údajov IS

1. Zodpovedné osoby sú povinné systematicky zálohovať údaje IS, vrátane prípadných detašovaných pracovísk.
2. Záložné kópie údajov IS sa vytvárajú denne, na záver, resp. po ukončení pracovnej doby. Navyše vytvárajú záložné kópie vybraných údajov (účtovníctvo a pod.) tak, aby zachytili stav pred pravidelnou uzávierkou.
3. Médiá, na ktorých sú uložené denné záložné kópie, je potrebné obmieňať minimálne v týždennom cykle (teda tak, aby v každom okamihu boli zálohované údaje minimálne z piatich po sebe nasledujúcich pracovných dní). Naviac je potrebné udržiavať aj záložné kópie z posledného pracovného dňa minimálne troch po sebe nasledujúcich mesiacov.
4. Zodpovedné osoby sú povinné zálohovať aj kompletný systém servera tak, aby bolo možné v prípade potreby rýchlo obnoviť základné a aplikačné programové vybavenie, konfiguračné súbory, štruktúru súborového systému a všetky podstatné parametre systému potrebné pre rutinnú prevádzku.
5. Média so záložnými kópiami údajov a systému je nevyhnutné skladovať tak, aby boli chránené pred neoprávnenou manipuláciou a nepriaznivými vplyvmi prostredia a aby sa zmenšilo riziko súčasného poškodenia alebo zničenia ako originálnych, tak aj záložných kópií chránených údajov
6. Všetky média so záložnými kópiami údajov a programového vybavenia musia byť označené tak, aby označenie jednoznačne určovalo aktuálny obsah média a taktiež aby bolo možné určiť dátum vytvorenia záložnej kópie na predmetnom médiu.

Článok 6
Zásady riešenia nepredvídaných udalostí s dopadom na prevádzku alebo údaje IS

1. V prípade nepredvídanej situácie ohrozujúcej prevádzku IS, alebo údaje IS sú zodpovedné osoby povinné pri riešení súvisiacich problémov zaistiť primeranú ochranu všetkých komponentov systému obsahujúcich citlivé údaje IS pred prístupom neoprávnených osôb.
2. V prípade nepredvídanej situácie je starosta obce oprávnený vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre riešenie udalosti.
3. Pri odstraňovaní následkov nepredvídaných situácií je starosta obce oprávnený stanoviť prioritu poradia riešenia problémov.

Článok 7
Zásady riešenia bezpečnostných incidentov

1. V prípade výskytu bezpečnostného incidentu zodpovedný zamestnanec bezodkladne informuje starostu obce s ktorým tiež konzultujú postup riešenia incidentu.
2. Riešenie každého bezpečnostného incidentu musí byť primerane zdokumentované. Dokumentuje sa predovšetkým príčina vzniku incidentu (pokiaľ je známa), dôsledky, všetky opatrenia prijaté pri riešení incidentu a ich účinnosť.
3. Zodpovedné osoby sa pri riešení bezpečnostného incidentu riadia nasledovnými prioritami:

a) bezodkladné obnovenie bežnej prevádzky IS aspoň v redukovanom režime, zabezpečenie ochrany údajov IS, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu,
b) zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu,
c) určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov,
d) zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu.

Článok 8
Prevencia

1. Informatici sú povinní pravidelne každý mesiac vykonať základnú preventívnu kontrolu kľúčových komponentov IS (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapĺňania pamäťovej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, previerka na výskyt nových programov v systéme, vyčistenie komponentov systému a pod.). Na tento účel je Informatik oprávnený vyhlásiť odstávku systému na nevyhnutne potrebnú dobu. Termín odstávky stanoví tak, aby čo najmenej narušil bežnú činnosť úradu a používateľov o tomto termíne oboznámi s dostatočným predstihom.
2. Zodpovedné osoby sú povinní pravidelne, minimálne raz za štvrťrok, vykonať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, média so záložnými kópiami údajov a programov, aktuálnosť zálohovaných prístupových hesiel a ďalších uchovávaných parametrov systému).

Článok 9
Záverečné ustanovenia

4. Porušenie tejto smernice bude posudzované ako závažné porušenie pracovnej disciplíny zamestnanca v zmysle príslušných ustanovení Zákonníka práce resp. zákona č.552/2003 Z.z. o výkone prác vo verejnom záujme.
5. Táto smernica nadobúda účinnosť dňom 10.01.2015

4. Havarijný plán informačného systému obce

Havarijný plán informačného systému obce Kysta (ďalej len ”havarijný plán”) špecifikuje základný postup pre prípad mimoriadnej situácie s negatívnym vplyvom na informačný systém obce a sprostredkovane na chod informačného systému Obecného úradu v Kyste
Havarijný plán pozostáva z havarijných procedúr, ktoré predstavujú súbor konkrétnych činností potrebných k zabezpečeniu kontinuity, prípadne k obnove funkcie IS obce. V havarijnom pláne sú stanovené zásady postupu pre prípady zlyhania kľúčových komponentov systému, neprítomnosti kľúčových zamestnancov (správcov systému), poškodenia údajov alebo kľúčových komponentov systému, podozrenia na zneužitie oprávnení a zistenia úmyselného útoku na systém. Ďalej sú v havarijnom pláne stanovené základné priority pre prípady práce IS obce v redukovanom (obmedzenom) režime, t.j. pri nedostatočnom objeme výpočtových, pamäťových a komunikačných kapacít.

Cieľ havarijného plánu

Hlavným cieľom havarijného plánu je zabezpečiť integritu systému a údajov Obecného úradu v Kyste a obcou zriadených organizačných útvarov v čase, keď je informačný systém alebo jeho časť nefunkčná.
Medzi ďalšie ciele havarijného plánu patria :

- zavedenie pocitu bezpečnosti do informačného systému,
- minimalizovanie času potrebného na zotavenie,
- garantovanie pripravenosti záložného riešenia,
- poskytnutie pravidiel pre testovanie plánov,
- minimalizovanie prijímania rozhodnutí v čase narušenia.

Definovanie havarijného stavu (kritickej situácie)

Vychádzajúc zo zoznamu rizík je potrebné zadefinovať havarijný stav. Je úlohou havarijného tímu, aby stanovil, v ktorých prípadoch je potrebné, aby sa pristúpilo k realizácii havarijných procedúr, prípadne v ktorých situáciách už havarijné procedúry nie je účelné aplikovať. Udalosti, ktoré svojim rozsahom môžu viesť k aktivovaniu niektorých procedúr havarijného plánu:

- požiar budovy alebo miestnosti s kľúčovými komponentmi IS OcÚ,
- vytopenie,
- zemetrasenie,
- výbuch,
- dlhodobé výpadky energetických zdrojov,

- dlhodobé výpadky dôležitých technických prostriedkov,
- plošné napadnutie pracovných staníc nebezpečným vírusom,
- zahltenie informačného systému,
- výpadky softvérových prostriedkov,
- poškodenia údajov,
- podozrenia na zneužitie oprávnení,
- zistenia úmyselného útoku na systému,
- hromadný výpadok ľudských zdrojov zabezpečujúcich prevádzku IS obce.

Definovanie oblasti pokrytia havarijným plánom

Pre účely havarijného plánu sú kľúčové komponenty IS obce tie technické a programové prostriedky a dokumenty, ktorých poškodenie, zlyhanie alebo neoprávnená manipulácia nimi môže mať za následok ohrozenie spoľahlivej a bezpečnej prevádzky IS obce. Medzi kľúčové komponenty IS obce patrí:

- pracovná stanica PCS01 v kancelárii starostu
- pracovná stanica PCS02 v kancelárii obecného úradu
- router pre pripojenie PCS02 k internetu
- záložný zdroj (UPS) pracovných staníc,
- systémové a aplikačné programové vybavenie používané v rámci IS,
- pamäťové média obsahujúce záložné kópie údajov IS,
- inštalačné média pre základné a aplikačné programové vybavenie IS,
- zoznam prístupových hesiel pre použitie v prípade neprítomnosti správcu systému.

Oprávnenie pre vstup do miestností s kľúčovými komponentmi

Prístup ku kľúčovým komponentom IS majú len starostovia obcí. Iné osoby majú prístup povolený len v prítomnosti starostu. Samostatne len so súhlasom povereného zamestnanca alebo starostu obce.

Pre vstup do priestorov, kde sú uložené kľúčové komponenty IS obce je potrebné dodržiavať kľúčový režim.

<u>Zoznam miestností s kľúčovými komponentmi:</u>

- kancelária obecného úradu

DÔLEŽITÉ INFORMÁCIE

a) V prípade požiaru v miestnostiach s kľúčovými komponentmi je potrebné postupovať aj v súlade s Požiarnym štatútom obce Požiarnym evakuačným plánom obce

b) Zoznam komponentov, dokumentov a nástrojov potrebných na riešenie kritickej situácie:
- záložné kópie údajov a softvéru sú uložené v plechovej skrini v kancelárii OcÚ,
- heslá správcu systému a aplikácií sú uložené v plechovej skrini v kancelárii OcÚ,
- náhradné kľúče od miestností s kľúčovými komponentmi sú uložené v kanc. OcÚ

c) Zoznam členov havarijného tímu, ktorí realizujú činnosti obsiahnuté v havarijnom pláne v čase narušenia kritických funkcií IS obce Kysta je uložený v plechovej skrini v kancelárií OcÚ

Prácu havarijného tímu riadi poverený zamestnanec : starosta obce

Meno a priezvisko : Adresa : č. tel. domov : Mobil : 0911 771 675

Mgr. Helena Borčíková, Kysta , Hlavná 44,

d) Zoznam externých dodávateľov služieb (oblasť služieb a kontaktné údaje), ktorí môžu, resp. budú participovať na riešení kritickej situácie pre:

1. **poskytovateľ pripojenia k internetu**
   - T – COM adresa Slovak Telekom, a.s. Bajkalska 28, 817 28 Bratislava
2. **poskytovateľ počítačových služieb (správa, údržba a opravy IS)**
   Secomp, s.r.o. adresa: M.R.Štefanika 49, 075 01 Trebišov

Stanovenie priorít obnovenia funkčnosti IS

Pre prípad narušenia IS obce je dôležité stanoviť v akej postupnosti sa bude vychádzať v procese obnovy chodu narušeného systému. Pre odstraňovanie kritickej situácie je potrebné stanoviť obnovovacie etapy pre nasledovné oblasti:

1. etapa - obnovenie funkčnosti operačných systémov, databázových systémov a aplikačného programového vybavenia:
   a) pracovná stanica v kancelárii starostu
   b) pracovná stanica v kancelárii obecného úradu
2. etapa - obnovenie pripojenia k internetu
3. etapa - obnovenie ostatných procesov.

Postup riešenia kritickej situácie

1. zvolanie členov havarijného tímu,
2. zistenie rozsahu poškodenia aktív IS (budova, miestnosti, technika a pod.),
3. zváženie danej situácie a určenie metodiky postupu odstránenia kritickej situácie,
4. spracovanie rozpisu zásahov pre členov havarijného tímu,
5. pri plošnom napadnutí vírusom informovať vyššie uvedené organizácie o kritickej situácii a pri jej odstraňovaní postupovať aj podľa metodických pokynov zmluvne dohodnutej firmy,

6. zabezpečiť finančné zdroje na obnovu pôvodného stavu,
7. zabezpečiť rekonštrukciu poškodených miestností s kľúčovými komponentmi systému (stavebné úpravy, maliarske práce, rozvody a pod.),
8. zabezpečiť zariadenie miestností s kľúčovými komponentmi systému (podlahové krytiny, nábytok, kancelárske potreby a pod.),
9. inštalácia techniky pre obnovu (pracovné stanice, periférne zariadenia, komunikačné prostredie a pod.),
10. obnova operačných systémov, databáz, aplikácií a údajov,
11. otestovanie funkčnosti obnoveného stavu,
12. presmerovanie prevádzky z havarijného stavu do obnoveného pôvodného stavu.

Zdokumentovanie kritickej situácie

Zdokumentovanie vzniknutia a riešenia kritickej situácie vykonajú poverení zamestnanci. Každý incident je potrebné zdokumentovať v prílohe havarijného plánu. O dočasných obzvlášť závažných, resp. núdzových opatrení poverený zamestnanec informuje starostu obce.

Minimálne údaje, ktoré musia byť zdokumentované:

a) dátum a čas výskytu zaznamenávanej udalosti,
b) stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti,
c) popis postupu riešenia,
d) jednoznačná identifikácia osoby, ktorá vykonala záznam.

Poskytovanie informácií

Informácie počas riešenia a po vyriešení kritickej situácie masmédiam poskytuje starosta obce.

TESTOVANIE HAVARIJNÉHO PLÁNU

Testovanie havarijného plánu je proces, na základe ktorého sa overí funkčnosť a aktuálnosť havarijného plánu a pripravenosť zamestnancov na riešenie kritickej situácie. Aby mohol byť havarijný plán úspešný pri použití počas kritickej situácie, je potrebné zapracovať doň všetky zmeny vyplývajúce z výsledkov testovania. Testovanie havarijného plánu vykoná havarijný tím raz za 12 mesiacov.

Aktualizácia havarijného plánu

Aktualizácia havarijného plánu je proces, pri ktorom sa do havarijného plánu zapracujú zmeny vyplývajúce zo zmien v štruktúre organizácie, personálnom zabezpečení, zmeny v informačnom systéme (hardvér, softvér alebo pri zmene priorít), zmeny vyplývajúce z testovania havarijného plánu a pod.

Poznámka

Dátumy aktualizácie, testovania a aktivácie havarijného plánu sa uvádzajú v prílohe havarijného plánu.

Záverečné ustanovenie

1. Porušenie ustanovení Bezpečnostného projektu bude posudzované ako závažné porušenie pracovnej disciplíny zamestnanca obce v zmysle príslušných ustanovení Zákonníka práce, resp. zákona č. 552/2003 Z. z. o výkone prác vo verejnom záujme v znení neskorších predpisov.
2. Tento vnútorný predpis nadobúda účinnosť dňom 10.01.2015.

.....
Mgr. Helena Borčíková
starostka obce