KIBERNETIČKA SIGURNOST U PAMETNIM GRADOVIMA

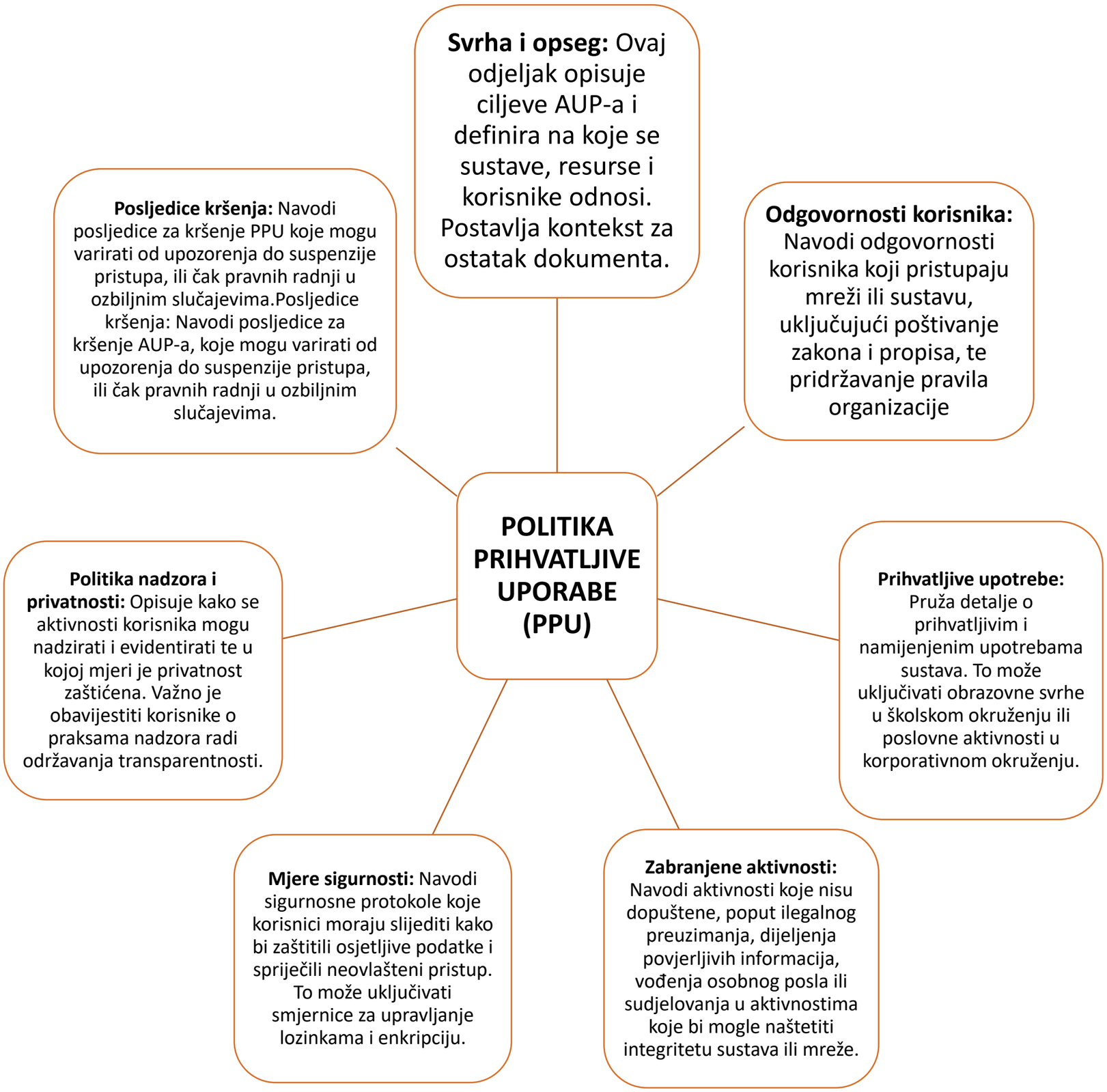
što trebamo učiniti

(praktični vodič)


POLITIKE POTREBNE ZA PROVEDBU KIBERNETIČKE SIGURNOSTI
Politika sigurnosti mreže: Definira strategije i tehnologije koje se koriste za zaštitu integriteta, povjerljivosti i dostupnosti mreže, uključujući vatrozide, sustave za otkrivanje upada i segmentaciju
Politika daljinskog pristupa: Upravlja načinom na koji zaposlenici mogu sigurno pristupati mreži i resursima organizacije s udaljenih lokacija, često uključujući korištenje VPN-a i višefaktorske autentifikacije
Politika prihvatljive upotrebe:Definira prihvatljive i neprihvatljive načine korištenja IT sredstava i resursa organizacije, postavljajući temeljna pravila za ponašanje korisnika.
Politika kontrole pristupa: Opisuje tko ima pristup specifičnim podacima i sustavima te koji je nivo pristupa dopušten, naglašavajući princip minimalnih privilegija.
Politika odgovora na incidente: Pruža okvir za reagiranje na kibernetičke incidente, uključujući uloge, odgovornosti i postupke za otkrivanje, suzbijanje, eliminaciju, oporavak i učenje iz incidenata.
Politika zaštite podataka i privatnosti: Osigurava da se podaci prikupljaju, obrađuju, pohranjuju i dijele u skladu s relevantnim zakonima i propisima o privatnosti, te da su uspostavljeni mehanizmi za zaštitu osjetljivih podataka.
Politika lozinki: Postavlja smjernice za kreiranje, korištenje i upravljanje lozinkama, uključujući kompleksnost, isteka i odgovornost korisnika
Politika upravljanja promjenama: Utvrđuje protokole za upravljanje promjenama u IT sustavima kako bi se smanjili rizici i utjecaj na poslovanje.
Politika sigurnosnih kopija i oporavka nakon katastrofe: piše postupke za izradu sigurnosnih kopija podataka i oporavak u slučaju gubitka podataka ili katastrofe kako bi se osigurala kontinuitet poslovanja.
Politika obuke i svijesti: Propisuje redovnu obuku o kibernetičkoj sigurnosti za zaposlenike kako bi ih informirala o potencijalnim prijetnjama i sigurnim praksama.
Politika upravljanja dobavljačima: Definira kako se treće strane dobavljači ocjenjuju, odabiru i upravljaju kako bi se osiguralo da se pridržavaju standarda kibernetičke sigurnosti organizacije.
Politika DVU (Donesi vlastiti uređaj): Regulira kako zaposlenici mogu koristiti svoje osobne uređaje u radne svrhe, osiguravajući da ti uređaji ispunjavaju sigurnosne standarde..
Politika upravljanja zakrpama: Uspostavlja proces za redovito ažuriranje softvera i sustava kako bi se zaštitili od ranjivosti i osigurala sigurnost sustava..
Politika e-pošte i komunikacije: Pruža smjernice za sigurnu upotrebu korporacijske e-pošte i komunikacijskih alata kako bi se spriječili napadi poput phishinga i malvera.


KIBERNETIČKA HIGIJENA
Instalirajte i koristite antivirusni softver: Koristite ugledni antivirusni i anti-malware softver za otkrivanje i uklanjanje prijetnji s vaših uređaja.
Budite oprezni s phishing prevarama: Educirajte se o prepoznavanju phishing pokušaja koji vas mamiti da otkrijete osjetljive informacije.
Ograničite osobne informacije koje dijelite online: Budite oprezni s osobnim informacijama koje dijelite na društvenim mrežama i drugim online platformama.
Redovito pratite svoje račune: Često provjeravajte svoje bankovne i kreditne kartice za bilo kakve neovlaštene transakcije.
Izradite sigurnosne kopije svojih podataka: Redovito izrađujte sigurnosne kopije važnih podataka na vanjski tvrdi disk ili mrežnu uslugu kako biste spriječili gubitak podataka u slučaju cyber incidenta.
Koristite snažne lozinke: Izradite složene lozinke koje uključuju kombinaciju slova, brojeva i posebnih znakova. Izbjegavajte korištenje lako pogodivih informacija, poput datuma rođenja ili uobičajenih riječi.
Omogućite dvostruku autentifikaciju (2A): Gdje god je to moguće, koristite 2A kako biste dodali dodatni sloj sigurnosti svojim računima.
Držite softver ažuriranim: Redovito ažurirajte svoje operacijske sustave, aplikacije i antivirusni softver kako biste se zaštitili od ranjivosti i prijetnji.
Budite oprezni s e-poštom i poveznicama: Ne otvarajte e-poruke od nepoznatih pošiljatelja i budite oprezni pri klikovanju na poveznice ili preuzimanju privitaka iz sumnjivih izvora.
Koristite sigurnu Wi-Fi vezu: Provjerite je li vaša Wi-Fi mreža zaštićena jakom lozinkom. Izbjegavajte korištenje javnog Wi-Fi-a za privatne transakcije.

U NASTAVKU SE DETALJNO NAVODE UPUTE ZA SVAKU OD POLITIKA PROVOĐENJA KINERNETIČKE SIGURNOSTI



POLITIKA KONTROLE PRISTUPA

Politika kontrole pristupa je ključni sigurnosni dokument u svakoj organizaciji, koji definira kako se odobrava i upravlja pristupom informacijama i resursima. Evo detaljnog pregleda što takva politika obično uključuje:

Svrha

- **Cilj**: Opišite svrhu politike, naglašavajući važnost zaštite kritičnih podataka i resursa od neovlaštenog pristupa.
- **Opseg**: Definirajte granice politike, uključujući sustave, podatke, aplikacije i korisničke grupe na koje se primjenjuje.

Definicije

- **Kontrola pristupa**: Mehanizmi i metode koje upravljaju dopuštenjima za korisnike da pristupe resursima.
- **Korisnici**: Osobe ili entiteti kojima je odobren pristup (zaposlenici, izvođači, partneri).
- **Resursi**: Podaci, aplikacije, sustavi i mreže zaštićene ovom politikom.

Izjave politike

- **Princip minimalnih privilegija**: Korisnici trebaju imati minimalni nivo pristupa potreban za obavljanje svojih dužnosti.
- **Pravo na znanje**: Pristup se odobrava isključivo na temelju trenutnih radnih odgovornosti korisnika.
- **Kontrola pristupa temeljena na ulogama (RBAC)**: Definirajte uloge unutar organizacije i dodijelite pristup na temelju tih uloga.
- **Odvajanje dužnosti**: Implementirajte kontrole za sprječavanje sukoba interesa i prijevara razdvajanjem zadataka među različitim korisnicima.

Mehanizmi kontrole pristupa

- **Autentifikacija**: Metode korištene za provjeru identiteta korisnika (npr., lozinke, biometrika, višefaktorska autentifikacija).
- **Autorizacija**: Postupci za dodjelu i provedbu dopuštenja (npr., RBAC, kontrola pristupa temeljena na atributima).
- **Revizija**: Bilježenje i praćenje pristupa kako bi se identificirali i odgovorili na neprimjerene pokušaje pristupa.

Odgovornosti korisnika

- Osigurati integritet i sigurnost korisničkih vjerodajnica.
- Prijavljivati bilo kakav sumnjiv pristup ili sigurnosne incidente.
- Redovito pregledavati i ažurirati dopuštenja za pristup.

Odgovornosti administratora

- Upravljati i provoditi politiku kontrole pristupa u cijeloj organizaciji.
- Provoditi redovite revizije i procjene kako bi se osigurala usklađenost.
- Implementirati i održavati tehnička rješenja koja podržavaju kontrolu pristupa.

Postupci kontrole pristupa

- **Dodjela korisnika**: Koraci za odobravanje, izmjenu i oduzimanje pristupa korisnicima.
- **Zahtjevi za pristup i odobrenje**: Postupak za traženje pristupa, uključujući potrebna odobrenja.
- **Periodični pregledi pristupa**: Rutinski pregledi za osiguranje nastavne nužnosti i prikladnosti privilegija pristupa.

Provedba i izuzeci

- Opišite korake za postupanje u slučaju kršenja politike, uključujući disciplinske mjere.
- Postupak za odobravanje iznimaka u politici, uključujući potrebna odobrenja i dokumentaciju.

Pregled i izmjena

- Raspored za pregled i ažuriranje Politike kontrole pristupa kako bi se adresirali novi prijetnje ili promjene u organizaciji.
- Dodijelite odgovornost za održavanje politike.

Podrške politike i dokumentacija

- Upućivanja na povezane politike kao što su Politika sigurnosti informacija, Politika zaštite podataka i Politika odgovora na incidente.

Usklađenost i pravni zahtjevi

- Osigurati usklađenost s relevantnim zakonima i pravilnicima kao što su GDPR, HIPAA ili drugi specifični standardi u industriji.

POLITIKA ODGOVORA NA INCIDENTE

Politika odgovora na incidente je ključni dokument za svaku organizaciju, koji opisuje kako otkriti, reagirati i oporaviti se od kibernetičkih incidenata. Evo općeg pregleda što takva politika može uključivati:

Uloge i odgovornosti
- Tim za odgovor na incidente: Identificirati članove tima i njihove specifične uloge tijekom incidenta, poput vođe tima, koordinatora komunikacije i tehničkih stručnjaka.
- Zaposlenici: Opišite odgovornosti svih zaposlenika u prijavljivanju i reagiranju na incidente.

Klasifikaciju incidenata
- Definirajte kriterije za klasifikaciju incidenata na temelju ozbiljnosti i utjecaja, poput niskog, umjerenog i visokog.

Faze odgovora na incidente
- Priprema: Opišite mjere za pripremu organizacije, uključujući obuku i resurse.
- Identifikacija: Utvrdite kako prepoznati i procijeniti potencijalne incidente.
- Suzbijanje: Opišite korake za ograničavanje štete i sprječavanje daljnjeg utjecaja.
- Eliminacija: Detaljno navedite kako ukloniti uzrok incidenta.
- Oporavak: Pružite smjernice za vraćanje sustava i usluga u normalno stanje.
- Naučene lekcije: Naglasite važnost pregledavanja incidenta radi poboljšanja budućih napora odgovora.

Plan komunikacije
Opišite kako će se informacije o incidentu komunicirati interno i eksterno, uključujući pravne i usklađene obveze.

Izvještavanje i dokumentacija
Detaljno navedite postupak za dokumentiranje pojedinosti incidenta i njihovo izvještavanje pravim stranama, kako tijekom, tako i nakon incidenta.

Usklađenost i pravni aspekti
Osigurajte da politika bude usklađena s relevantnim zakonima, propisima i industrijskim standardima.

Obuka i svijest
Definirajte zahtjeve za redovitu obuku i programe svijesti kako bi se zaposlenici informirali o politici i postupcima.
Pregled i ažuriranje: Odredite učestalost i postupak za pregled i ažuriranje politike kako bi se osiguralo da ostane učinkovita i relevantna.

POLITIKA ZAŠTITE PODATAKA I PRIVATNOSTI

POLITIKA LOZINKI

Politika jakih lozinki je ključna za zaštitu osjetljivih informacija i osiguranje sigurnosti. Evo nekoliko uobičajenih preporuka za robustnu politiku lozinki:

Minimalna duljina: Lozinke bi trebale biti dugačke najmanje 12-16 znakova.

Složenost: Uključite mješavinu velikih i malih slova, brojeva i posebnih znakova (npr., @, #, $, %, itd.).

Izbjegavanje uobičajenih riječi: Izbjegavajte uobičajene riječi, lako pogađane informacije (poput "lozinka", "123456" ili vašeg imena) te nizove ili ponavljajuće znakove (poput "abcd" ili "1111").

Izbjegavajte osobne informacije: Ne koristite lako dostupne osobne informacije poput rođendana, imena članova obitelji, ljubimaca itd.

Jedinstvene lozinke: Koristite različite lozinke za različite račune kako biste spriječili da kompromitiranje jednog računa ugrozi druge.

Redovita promjena: Redovito mijenjajte lozinke, iako se ovaj savjet može razlikovati ovisno o kontekstu i drugim mjerama sigurnosti.

Višefaktorska autentifikacija (MFA): Gdje je moguće, koristite MFA za dodatni sloj sigurnosti iznad lozinke.

Upravitelji lozinki: Koristite upravitelj lozinki za sigurno pohranjivanje i upravljanje vašim lozinkama.

Zaključavanje računa: Implementirajte mehanizam zaključavanja računa kako biste se zaštitili od napada "brute force", koji zaključava račun nakon nekoliko neuspješnih pokušaja prijave.

Enkripcija: Pohranjujte lozinke korištenjem jakih metoda enkripcije i izbjegavajte pohranu lozinki u običnom tekstu.

POLITIKA DALJINSKOG PRISTUPA

Politika daljinskog pristupa je skup pravila i smjernica dizajniranih za upravljanje načinima na koje zaposlenici ili ovlašteni korisnici mogu povezivati se s mrežnim resursima tvrtke iz udaljenih lokacija. Ova politika pomaže osigurati sigurnost i cjelovitost podataka i sustava koji se pristupaju na daljinu. Evo nekih ključnih komponenti koje se obično uključuju u politiku daljinskog pristupa:

Svrha. Objasnite zašto je politika nužna i što želi postići, kao što su zaštita osjetljivih informacija i osiguravanje sigurnog pristupa resursima tvrtke.
Opseg. Definirajte na koga se politika odnosi, poput zaposlenika, izvođača i trećih strana, te na koje sustave ili podatke se primjenjuje.

Metode pristupa. Specificirajte odobrene metode za daljinski pristup, poput VPN-a, sigurnih web portala ili specifičnih aplikacija udaljene radne površine.
Autentifikacija. Opišite mehanizme autentifikacije koji su potrebni, poput višefaktorske autentifikacije (VA), jakih lozinki i korisničkih ID-eva, kako bi se potvrdio identitet korisnika.

Zahtjevi za uređaje. Navedite sigurnosne mjere koje moraju biti prisutne na bilo kojem uređaju koji se koristi za daljinski pristup, kao što su ažuriran antivirusni softver, vatrozidi i sigurnosne zakrpe.

Zaštita podataka. Opišite kako bi podaci trebali biti zaštićeni tijekom prijenosa i pohrane, poput korištenja enkripcije ili ograničavanja mogućnosti preuzimanja.
Odgovornosti korisnika. Definirajte odgovornosti korisnika, uključujući zaštitu vjerodajnica, odjavljivanje kada se ne koristi i prijavljivanje izgubljenih ili ukradenih uređaja.

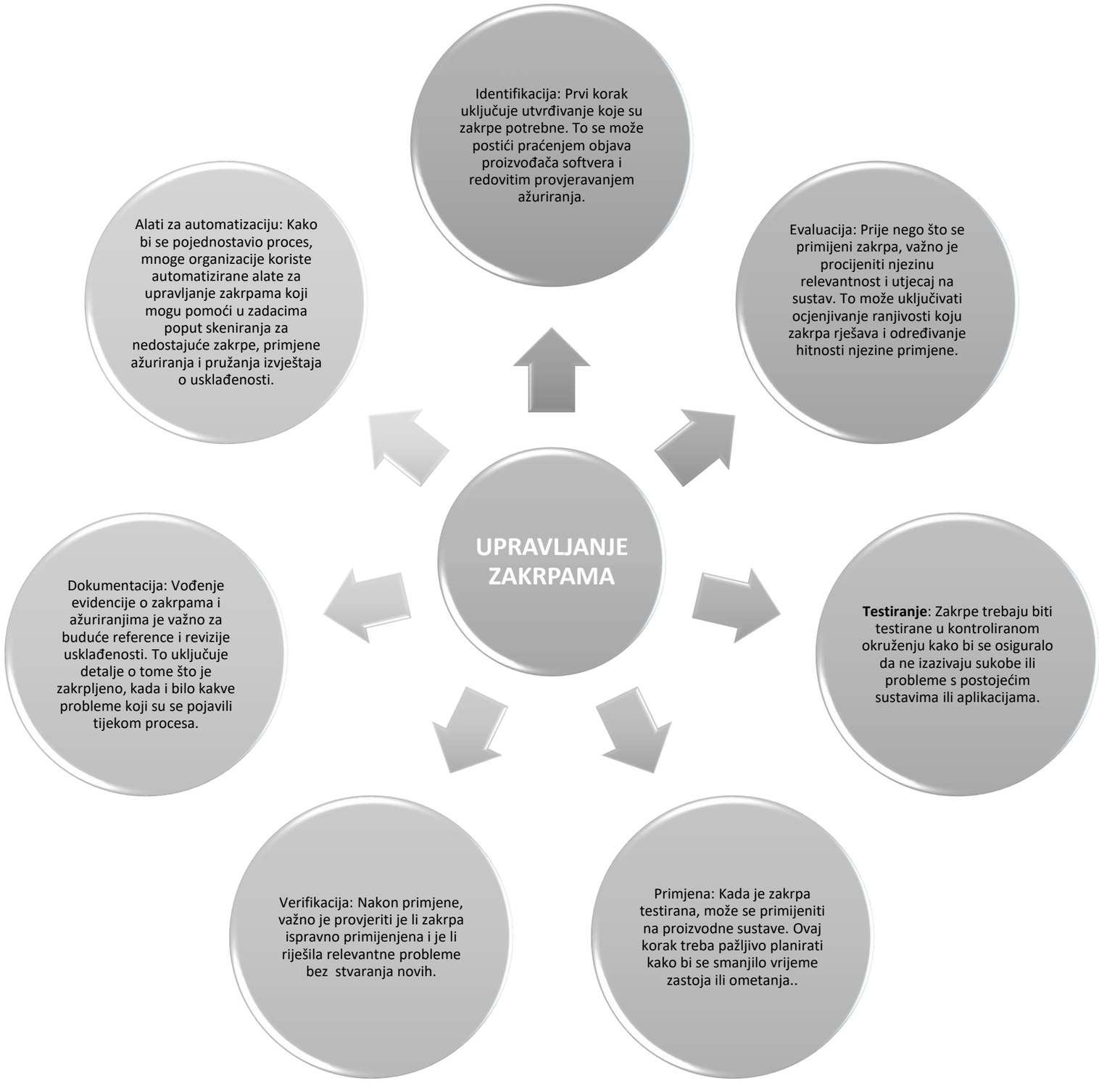
Praćenje i bilježenje. Naznačite da se sve aktivnosti daljinskog pristupa mogu pratiti i bilježiti u svrhu sigurnosti i usklađenosti.

Usklađenost i provedba. Opišite moguće disciplinske mjere za nepoštivanje politike, do uključivanja otkaza zaposlenju ili ugovoru.

Pregled i ažuriranje. Navedite koliko često će se politika pregledavati i ažurirati kako bi se pratili tehnološki i poslovni promjene.


POLITIKE MREŽNE SIGURNOSTI
Kontrola pristupa: Definira tko ima pravo pristupa različitim dijelovima mreže i razinu dodijeljenog pristupa. Često uključuje protokole za verifikaciju identiteta, autorizaciju i kontrole pristupa temeljene na ulogama.
Revizija i održavanje politike: Opisuje proces redovite revizije i ažuriranja politike kako bi se prilagodila novim prijetnjama i tehnološkim promjenama.
Prihvatljiva upotreba: Opisuje prihvatljive i neprihvatljive aktivnosti za korisnike na mreži, osiguravajući da se resursi koriste etički i legalno.
Obuka o sigurnosti: Specifikacija zahtjeva za redovnu obuku i programima podizanja svijesti kako bi se osiguralo da svi korisnici razumiju svoje uloge u održavanju sigurnosti mreže.
Zaštita podataka: Ocrtava kako bi podaci trebali biti zaštićeni, i tijekom prijenosa i kada su pohranjeni, uključujući standarde enkripcije i postupke izrade sigurnosnih kopija.
Upravljanje prijetnjama: Identificira prijetnje i ranjivosti mreže te opisuje kako upravljati i ublažiti te rizike putem alata poput vatrozida, antivirusnog softvera i sustava za otkrivanje upada.
Odgovor na incidente: pruža plan kako odgovoriti na sigurnosne provale ili incidente, uključujući korake za zadržavanje, iskorjenjivanje i oporavak.
Praćenje mreže: Pruža informacije o tome kako će se mrežna aktivnost pratiti i bilježiti, te tko je odgovoran za provođenje ovih aktivnosti.

UPRAVLJANE ZAKRPAMA je proces distribuiranja i primjene ažuriranja softvera. Ova ažuriranja često se nazivaju "zakrpama". Cilj upravljanja zakrpama je osigurati da su sustavi i aplikacije ažurni i sigurni.



POLITIKA ELEKTRONIČKE POŠTE I KOMUNIKACIJE

Svrha
Svrha ove politike je pružiti smjernice za prikladnu upotrebu e-pošte i komunikacijskih alata unutar organizacije kako bi se osigurala učinkovita komunikacija, sigurnost podataka i profesionalnost.

Opseg
Ova politika se odnosi na sve zaposlenike, izvođače i treće strane koji koriste e-mail i komunikacijske sustave organizacije.

Opće smjernice

- **Profesionalni ton**: Sve komunikacije trebaju se provoditi na profesionalan način. Koristite pristojan jezik, pravilnu gramatiku i odgovarajuće formalnosti.
- **Jasnoća i sažetost**: Budite jasni i sažeti u svojim e-mailovima i porukama kako biste izbjegli nesporazume.
- **Naslovi**: Koristite opisne naslove koji točno odražavaju sadržaj e-pošte.

Upotreba e-pošte

- **Radna svrha**: E-pošta se prvenstveno treba koristiti za komunikaciju vezanu uz posao. Osobna upotreba treba biti svedena na minimum.
- **Povjerljivost**: Nemojte dijeliti osjetljive informacije ili povjerljive podatke putem e-pošte osim ako nisu enkriptirani ili sigurni.
- **Prilozi**: Ograničite priloge na potrebne datoteke i osigurajte da su skenirani na viruse prije slanja.

Vrijeme odgovora

- **Potvrda**: Ciljajte na to da potvrdite primitak e-pošte unutar 24 sata.
- **Na vrijeme**: Odgovorite na e-mailove vezane uz posao pravodobno, idealno unutar dva radna dana.

Komunikacijski alati

- **Prikladni kanali**: Koristite odabrane komunikacijske alate (npr. e-pošta, instant poruke, videokonferencije) na odgovarajući način, ovisno o prirodi komunikacije.
- **Sastanci**: Planirajte sastanke samo kada je to potrebno i osigurajte jasne dnevne redove unaprijed.

Društveni mediji i vanjska komunikacija

- **Predstavljanje organizacije**: Zaposlenici ne smiju otkrivati povjerljive informacije tvrtke na društvenim mrežama ili putem bilo koje vanjske komunikacije.
- **Osobni računi**: Jasno razlikujte osobne i profesionalne računa.

Posljedice kršenja politike
Nepridržavanje ove politike može rezultirati disciplinskim mjerama, uključujući otkaz zaposlenju.

Pregled politike
Ova politika će se pregledavati godišnje i ažurirati po potrebi kako bi odražavala trenutne potrebe organizacije.

Potvrda
Svi zaposlenici moraju potvrditi da su pročitali i razumjeli Politiku e-pošte i komunikacije.

POLITIKA DVU („DONESI VLASTITI UREĐAJ“)

Politika DVU je skup smjernica koje organizacije kreiraju kako bi upravljale upotrebom osobnih uređaja - poput pametnih telefona, tableta i prijenosnih računala - unutar radnog mjesta. Ključni ciljevi DVU politike uključuju povećanje produktivnosti, osiguranje sigurnosti i definiranje odgovornosti kako za zaposlenike, tako i za organizaciju. Evo nekih uobičajenih elemenata koje obično uključuje DVU politika:

1. **Svrha i ciljevi**: Objasnite svrhu politike i jasno naznačite ciljeve kao što su povećanje produktivnosti i osiguranje sigurnosti podataka.
2. **Opseg**: Definirajte koji zaposlenici ili grupe imaju pravo koristiti osobne uređaje i na koje sustave ili podatke se politika primjenjuje.
3. **Prihvaćeni uređaji**: Nabrojite koji su uređaji odobreni za korištenje (npr. određeni modeli pametnih telefona ili tableta) i operativni sustavi koji se smiju koristiti.
4. **Sigurnosni zahtjevi**: Opišite sigurnosne mjere koje moraju biti implementirane na osobnim uređajima, uključujući enkripciju, zaštitu lozinkama i ažuriranje softvera.
5. **Upravljanje podacima**: Definirajte kako se osjetljivi podaci trebaju pohranjivati i prenositi na osobnim uređajima. To može uključivati politiku sigurnosnih kopija i pristup mrežnim resursima.
6. **Odgovornosti korisnika**: Opišite odgovornosti zaposlenika u vezi s korištenjem osobnih uređaja, uključujući zaštitu vjerodajnica i obavještavanje o gubitku ili krađi uređaja.
7. **Politika korištenja aplikacija**: Utvrdite koje su aplikacije dozvoljene ili zabranjene na osobnim uređajima povezanima s radom.
8. **Praćenje i nadzor**: Obavijestite korisnike da organizacija može pratiti aktivnosti povezane s radom na osobnim uređajima radi sigurnosti i usklađenosti.
9. **Posljedice kršenja**: Opišite moguće disciplinske mjere za nepridržavanje politike, uključujući suspenziju ili ukidanje prava na korištenje osobnih uređaja.
10. **Pregled i ažuriranje**: Odredite učestalost i postupak za pregled i ažuriranje politike kako bi se prilagodila novim tehnologijama i poslovnim potrebama.

Implementacija DVU politike može pomoći u smanjenju sigurnosnih rizika, povećanju produktivnosti i pružanju jasnih smjernica zaposlenicima o korištenju osobnih uređaja u radnom okruženju.

POLITIKA UPRAVLJANJA DOBAVLJAČIMA

Okvir oblikovan za vođenje organizacije u upravljanju njenim odnosima s dobavljačima, izvršiteljima i pružateljima usluga. Ova politika opisuje procese i odgovornosti povezane s izborom dobavljača, evaluacijom, praćenjem i raskidom suradnje.

Svrha

- Definirati ciljeve politike upravljanja dobavljačima.
- Osigurati usklađenost s pravnim, regulatornim i najboljim praksama.

Opseg

- Specificirati odjele ili područja organizacije na koja se politika odnosi.
- Opišite tipove dobavljača koji su pokriveni (npr., dobavljači, pružatelji usluga).

Proces odabira dobavljača

- Kriteriji za odabir dobavljača (npr., kvalifikacije, iskustvo, kapacitet).
- Postupak za traženje ponuda ili cijena.
- Evaluacijska matrica ili kriteriji za procjenu ponuda.

Pripazivost (Due Diligence)

- Zahtjevi za provođenje pripazivosti (financijski, operativni, etički).
- Postupci procjene rizika.

Upravljanje ugovorima

- Smjernice za pregovaranje o ugovorima i odobravanje.
- Ključni elementi ugovora (npr., uvjeti, struktura plaćanja, ugovori o razini usluga).

Praćenje performansi

- Procesi za praćenje performansi dobavljača prema dogovorenim mjerama.
- Učestalost i tipovi pregleda performansi (npr., kvartalno, godišnje).

Komunikacija s dobavljačima

- Protokoli za redovnu komunikaciju s dobavljačima.
- Postupci za rješavanje problema ili zabrinutosti.

Upravljanje rizicima

- Identifikacija i upravljanje rizicima povezanima s odnosima s dobavljačima.
- Planiranje za neuspjeh dobavljača.

Usklađenost i izvještavanje

- Osigurati da dobavljači ispunjavaju relevantne zakone i propise.
- Struktura izvještavanja za probleme vezane uz dobavljače.

Prestanak odnosa s dobavljačima

- Uvjeti pod kojima se dobavljač može otkazati.
- Postupci za miran prekid i planiranje prijelaza.

Revizija i ažuriranje politike

- Učestalost pregleda politike (godišnje, polugodišnje).
- Postupci za ažuriranje politike prema potrebi.

Uloge i odgovornosti

- Definirajte uloge za pojedince ili timove uključene u upravljanje dobavljačima.
- Odgovornosti za nadzor, procjenu i izvještavanje.

POLITIKA OBUKE I OSVIJEŠTENOSTI

Cilj: Opišite ciljeve politike, kao što su osiguranje usklađenosti s propisima, promicanje sigurnog i produktivnog radnog okruženja te minimiziranje rizika.

Opseg: Definirajte na koga se politika odnosi, bilo da se radi o svim zaposlenicima, izvođačima ili specifičnim odjelima unutar organizacije.

Uloge i odgovornosti: Detaljno navedite tko je odgovoran za razvoj, implementaciju i održavanje programa obuke. To obično uključuje odjele za ljudske resurse, službenike za usklađenost i menadžere.

Zahtjevi za obuku: Navesti kakva je obuka potrebna, uključujući obvezne tečajeve, učestalost održavanja obuka i potrebne certifikate.

Sadržaj i isporuka: Opišite vrste obrazovnih materijala koji će se koristiti (npr. online tečajevi, radionice, seminari) i kako će se oni isporučivati.

Praćenje i evaluacija: Objasnite kako će se mjeriti učinkovitost obuke, putem procjena, anketa o povratnim informacijama ili mjernih pokazatelja performansi.

Dokumentacija i evidencija: Uspostavite procedure za održavanje evidencije svih obuka, prisutnosti i rezultata završetka.

Usklađenost i provedba: Detaljno navedite posljedice nepoštivanja zahtjeva za obuku, uključujući disciplinske mjere.

Stalno poboljšanje: Potaknite redovito pregledavanje i ažuriranje programa obuke kako bi ostali relevantni i učinkoviti.

Kampanje svijesti: Istaknite sve planirane inicijative za podizanje stalne svijesti, kao što su bilteni, e-mailovi ili plakati.

POLITIKA SIGURNOSNIH KOPIJA I OPORAVKA NAKON KATASTROFE

Sigurnosne kopije

Svrha: Sigurnosne kopije koriste se za izradu kopija podataka koje se mogu vratiti u slučaju da su izvorni podaci izgubljeni ili oštećeni.

Vrste sigurnosnih kopija:

- Potpuna sigurnosna kopija: Potpuna kopija svih podataka. Jednostavno je, ali može trajati dugo i zahtijeva više prostora za pohranu.
- Inkrementalna sigurnosna kopija: Kopiraju se samo podaci koji su se promijenili od posljednje sigurnosne kopije. Ovo je brže i štedi prostor za pohranu, ali može biti složenije za vraćanje.
- Diferencijalna sigurnosna kopija: Kopira sve promjene napravljene od posljednje potpune sigurnosne kopije. Nudi srednje rješenje između potpune i inkrementalne sigurnosne kopije.

Rješenja za sigurnosne kopije:

- **Lokalno:** Lokalna pohrana poput vanjskih tvrdih diskova ili mrežno povezane pohrane (NAS).
- **Temeljeno na oblaku:** Usluge poput AWS-a, Azure-a ili Google Clouda pružaju izvanmrežne sigurnosne kopije koje su skalabilne i sigurne.
- **Hibridno:** Kombinira lokalne i oblačne sigurnosne kopije za veću fleksibilnost i redundantnost.
- **Učestalost:** Rasporedi sigurnosnih kopija mogu se postaviti na dnevne, tjedne ili prema potrebama poslovanja. Kritični podaci moraju se kopirati na sigurnu lokaciju.

Oporavak nakon katastrofe

Svrha: Oporavak nakon katastrofe uključuje procese i tehnologije koje obnavljaju IT infrastrukturu i operacije nakon katastrofalnog događaja.

Komponente:

- **Plan oporavka nakon katastrofe (DRP):** Dokumentirani proces s detaljnim uputama o tome kako reagirati na neplanirane incidente.
- **Objektiv vremena oporavka (RTO):** Maksimalno prihvatljivo trajanje vremena koje aplikacija ili usluga može biti nedostupna nakon kvara.
- **Objektiv točke oporavka (RPO): Maksimalna količina gubitka podataka koju organizacija može podnijeti, obično mjerena vremenskim odmakom prije katastrofe.**

Strategije:

- **Oporavak temeljen na sigurnosnim kopijama:** Korištenje sigurnosnih kopija za vraćanje sustava.
- **Replikacija:** Održavanje kopije podataka u stvarnom vremenu na drugom mjestu.
- **Oporavak nakon katastrofe u oblaku:** Korištenje oblaka za brzo pokretanje rezervnih okruženja.

Testiranje: Redovito testiranje planova oporavka nakon katastrofe ključno je za osiguranje da oni funkcioniraju kako je zamišljeno i da su svi zaposlenici obučeni o svojim ulogama unutar plana.

Kontinuitet poslovanja: Osigurava da ključne funkcije mogu nastaviti s radom tijekom i nakon katastrofe, pružajući otpornost na niz scenarija.

POLITIKA UPRAVLJANJA PROMJENAMA

Svrha
Uspostaviti standardni pristup za upravljanje promjenama u sustavima, procesima i organizacijskim strukturama uz minimiziranje ometanja i osiguranje usklađenosti.

Opseg
Ova politika se odnosi na sve zaposlenike, izvođače i pružatelje usluga trećih strana koji su uključeni u aktivnosti vezane uz promjene unutar organizacije.

Definicije promjena: Svaka modifikacija sustava, procesa ili usluge koja može utjecati na organizaciju.

Zahtjev za promjenu: Formalni prijedlog za promjenu.

Savjetodavni odbor za promjene: Grupa dionika koja savjetuje o rangiranju promjena po važnosti i planiranju promjena.

Klasifikacija promjena

Promjene se mogu klasificirati kao:

- **Standarne promjene:** Pre-odobrene i niskorizične promjene koje slijede unaprijed određeni proces.
- **Normalne promjene:** Promjene koje zahtijevaju procjenu, odobrenje i planiranje
- **Hitne promjene:** Hitne promjene koje je potrebno brzo implementirati kako bi se minimalizirao utjecaj.

Proces promjena

1. **Identifikacija:** Prepoznavanje potrebe za promjenom.
2. **Podnošenje zahtjeva za promjenu:** Podnošenje formalnog zahtjeva za promjenu koji detaljno opisuje predložene promjene, razloge i procjenu utjecaja.
3. **Procjena i odobrenje:**
    - Pregled od strane CAB-a za normalne promjene.
    - Automatsko odobrenje za standardne promjene.
4. **Planiranje i implementacija:** Razvijanje plana za promjenu, uključujući vremenske okvire i resurse.
5. **Testiranje:** Validacija promjena u kontroliranom okruženju prije pune implementacije.
6. **Pregled i zatvaranje:** Evaluacija uspješnosti promjene i formalno zatvaranje zahtjeva za promjenu.

Dokumentacija

Sve promjene moraju biti dokumentirane, uključujući:

- Obrazac zahtjeva za promjenu
- Zapisi o odobrenju
- Planovi implementacije
- Rezultati pregleda nakon implementacije

Zainteresirane strane moraju biti informirane o promjenama koje utječu na njihov rad. Informacija mora biti jasna i pravovremena.

Obuka
Zaposlenici uključeni u proces upravljanja promjenama moraju imati odgovarajuću obuku kako bi učinkovito pridržavali ovu politiku.

Pregled i stalno poboljšanje
Ova politika će se pregledavati godišnje ili po potrebi kako bi se osigurala njena učinkovitost i relevantnost.

REFERENCE

European Commission. (2020). **The Directive on security of network and information systems (NIS directive)**. Retrieved from https://ec.europa.eu/digital-strategy/our- policies/nis-directive_en

European Union Agency for Cybersecurity (ENISA). (2023). **NIS2 Directive: A high common level of cybersecurity in the EU**. Retrieved from https://www.enisa.europa.eu/publications/the-nis2-directive

CISA. (2022). **EU NIS2 Directive: Understanding the new cybersecurity requirements**.Retrieved from https://www.cisa.gov/eu-nis2-directive

Republic of Croatia. (2018). **Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga** (Narodne novine 64/18).