CASE2026

Rijeka, ožujak 2026

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU U PAMETNIM GRADOVIMA PREMA NORMI ISO/IEC 27001

Damir Maleković, Željko Kovačević,
Aleksandar Stojanović, Maja Dabčević

01 Pametni gradovi

- Oslanjaju se na informacijsko-komunikacijske tehnologije kako bi unaprijedili kvalitetu života građana i učinkovitost javnih usluga.
- Uključuju velik broj heterogenih informacijskih rješenja, IoT uređaja i vanjskih pružatelja usluga, što značajno povećava sigurnosne rizike

02 Informacijska sigurnost / ISO/IEC 27001

- Sustavno upravljanje informacijskom sigurnosti je ključni preduvjet za pouzdano i sigurno korištenje informacija kojima organizacijske jedinice gradova raspolažu

03 Svrha rada

- Rad analizira mogućnosti primjene norme ISO/IEC 27001 kao okvira za uspostavu sustava upravljanja informacijskom sigurnosti u pametnim gradovima.
- Identifikacija ključnih izazova implementacije sustava
- Praktične preporuke za implementaciju ključnih zahtjeva / sigurnosnih kontrola

KONCEPT PAMETNOG GRADA

Pametni promet

- Pametna parkirališta
- Sigurnost lokacijskih podataka
- Autentikacija i šifriranje

Pametne komunalne mreže

- Pametna brojila
- Upravljanje energijom
- Zaštita IoT sustava

Javna sigurnost

- Centar za hitne slučajeve
- Zaštita snimki

Pametno obrazovanje

- e-učenje
- Podaci učenika

Senzorske mreže

- IoT infrastruktura
- Analitika i kontrola pristupa

Digitalne usluge

- e-uprava i portal građana
- Sigurnost baza podataka

Autentikacija i šifriranje

Pametno zdravstvo

- Medicinski podaci
- Povjerljivost informacija

KONCEPT PAMETNOG GRADA

- Barcelona - Decidim platforma omogućuje građanima sudjelovanje u odlukama o proračunu, urbanim projektima i lokalnim politikama putem online glasovanja.
- Barcelona - projekt „Smart Waste Management Barcelona”. U gradu su postavljeni spremnici za otpad opremljeni senzorima koji mjere popunjenost i automatski šalju podatke komunalnim službama, a na temelju tih informacija optimizira se ruta prikupljanja otpada, čime se smanjuje potrošnja goriva, emisija CO_2 i operativni troškovi.
- Helsinki – model „MaaS” koji kroz jedinstvenu digitalnu platformu integrira različite oblike prijevoza pa tako kroz aplikaciju Whim korisnici mogu planirati putovanje, rezervirati i platiti javni prijevoz, taksi usluge, unajmljivanje vozila ili bicikala.
- Singapore – naprednog upravljanje prometom na razini cijelog grada kroz sustav koji koristi digitalne tehnologije i analizu podataka u stvarnom vremenu kako bi regulirao prometne tokove, osobito u područjima s velikim prometnim opterećenjem.

STRUKTURNA OBILJEŽJA PAMETNIH GRADOVA I POTENCIJALNI PROBLEMI

- Heterogenost sustava - složeni sustav sustava, koji često uključuje neovisne komponente, a koje moraju efikasno surađivati (podaci iz različitih gradskih ureda, odjela i poduzeća, oblikuju digitalnu imovinu pametnih gradova koja zahtijeva pažljivo upravljanje)
- Izrazito dinamično okruženje - iznimno velike mreže senzora i podataka koji se nalaze pohranjeni u IT sustavima
- Fragmentirano upravljanje - pitanje granica odgovornosti za pojedine informacije između različitih gradskih ureda i odjela
- Osiguravanje vjerodostojnosti i integriteta informacija – GDPR i sl.
- Problem potencijalne interoperabilnosti i nekompatibilnosti različitih dijelova sustava
- Skalabilnost - složenost sustava autentifikacije, autorizacije i kontrole pristupa zbog velikog broja korisnika predstavlja potencijalni izazov

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

- Osnovna opasnost:
  - očuvanje sigurnosti informacija pohranjenih u sustavima pametnih gradova

- Upravljanje informacijskom sigurnošću - sustavan i metodološki strukturiran pristup zaštiti informacija te informacijskih sustava, kao i povezanih resursa od različitih oblika prijetnji koje mogu ugroziti njihovu povjerljivost, integritet i dostupnost.

- Na provedbenoj razini, obuhvaća upravljanje skupom različitih sastavnica kao što su organizacijski procesi, politike, edukaciju zaposlenika, upravljanje rizicima, ali i tehničke mjere, poput zaštite mreže ili kriptografije, kojom se čuva integritet i povjerljivost informacija s kojima poduzeće raspolaže.

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

- Temelj upravljanja informacijskom sigurnošću: prepoznavanje i procjena rizika
- Prilikom uspostave sustava upravljanja informacijskom sigurnošću očekuje se identifikacija tipova informacija koje organizacija posjeduje, gdje se one nalaze, tko im ima pristup i koje sve prijetnje mogu direktno ili indirektno utjecati na njihovu sigurnost.
- Važan aspekt upravljanja informacijskom sigurnošću je uspostava jasnih pravila i odgovornosti unutar same organizacije.

- Na temelju takve procjene rizika određuju se odgovarajuće sigurnosne mjere i aktivnosti koje mogu uključivati tehničke kontrole, administrativne procedure i organizacijske politike, a kojima se identificirani rizici smanjuju na prihvatljivu razinu kako bi se osiguralo stabilno i sigurno funkcioniranje organizacije koja uspostavlja takav sustav.

ISO/IEC 27001:2022

Općeprihvaćena metodologija

- 100.000 izdanih certifikata u svijetu
- prihvaćena u RH od strane HZNa u 2023.godini (HRN EN ISO/IEC 27001:2023)

Svrha

- Definira zahtjeve za uspostavu, implementaciju, održavanje i stalno poboljšavanje sustava upravljanja informacijskom sigurnošću.

Cilj

- Osigurati organizacijama strukturirani okvir za zaštitu informacija od različitih prijetnji, uključujući neovlašteni pristup, gubitak podataka, kibernetičke napade ili neovlaštene izmjene informacija.

Obilježje

- primjenjiva na organizacije svih veličina i sektora – od javne uprave i gradova, do privatnih tvrtki i tehnoloških organizacija, budući da se temelji na univerzalnim principima upravljanja rizicima i zaštite informacija.

SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU (ISMS) PREMA ISO 27001

➢ ISMS predstavlja skup politika, procedura, procesa i tehnoloških mjera koje organizacija koristi za upravljanje i zaštitu informacija.

➢ On obuhvaća:

- definiranje sigurnosne politike,
- upravljanje rizicima,
- dodjela odgovornosti,
- definiranje kontrole pristupa,
- edukaciju zaposlenika,
- upravljanje incidentima
- kontinuirano praćenje i poboljšavanje sigurnosnih mjera.

ISO/IEC 27001:2022

➢ Norma ISO/IEC 27001 sastoji se od deset poglavlja, a sadrži niz zahtjeva koji se odnose na uspostavu i održavanje procesa za razumijevanje konteksta organizacije, identifikaciju zainteresiranih strana i njihovih potreba te definiranje opsega ISMS-a.

➢Sadržaj norme ISO/IEC 27001:2022:

Poglavlja norme ISO/IEC 27001:2022	
1. Opseg primjene	6. Planiranje
2. Normativne reference	7. Podrška
3. Pojmovi i definicije	8. Operativno djelovanje
4. Kontekst organizacije	9. Procjena učinkovitosti
5. Vodstvo	10. Neprekidno unapređenje

ISO/IEC 27001:2022 I ISO/IEC 27002:2022

- ISO/IEC 27001 i ISO/IEC 27002 zajedno čine komplementarni par i primjenjuju se isključivo zajedno

- Norma ISO/IEC 27002 sadrži ukupno 93 kontrole podijeljene u četiri glavne teme:

- Organizacijske kontrole - upravljanje informacijskom sigurnošću, uloge i odgovornosti, upravljanje rizicima, usklađenost s propisima itd.

- Kontrole vezane uz ljude - sigurnost ljudskih resursa, obuka i svijest, postupci prilikom zapošljavanja i prestanka radnog odnosa, odgovornost zaposlenika za zaštitu informacija itd.

- Fizičke kontrole - kontrola pristupa objektima, zaštita opreme i uređaja, nadzor i zaštita fizičkih prostora gdje se obrađuju informacije itd.

- Tehničke kontrole - kontrola pristupa sustavima, kriptografija, sigurnost mreža i komunikacija, upravljanje informacijskim sustavima, sigurnost u razvoju i održavanju softvera itd.

ISO/IEC 27001:2022 I ISO/IEC 27002:2022

ISO/IEC 27001:2022

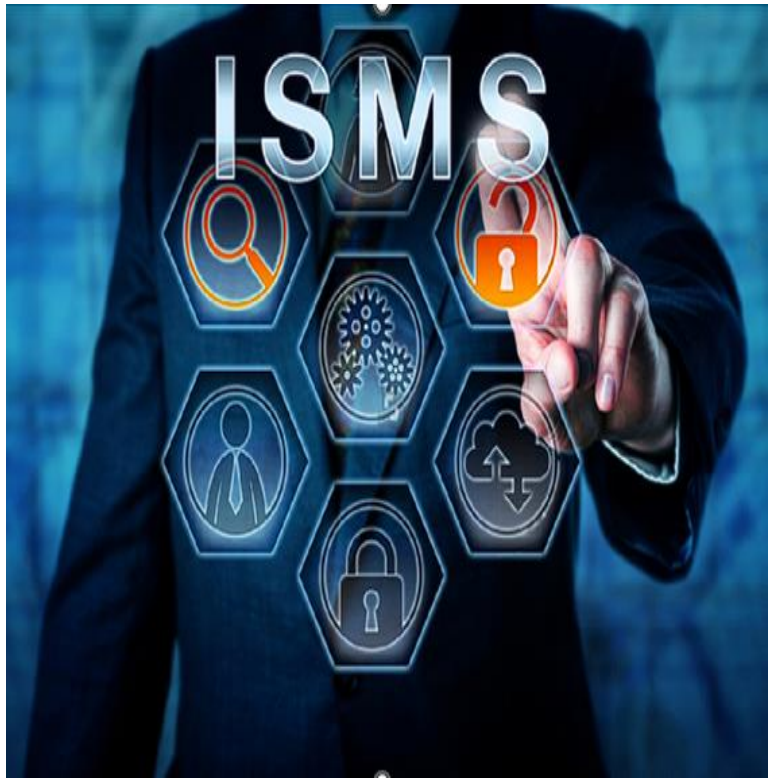
Postavlja zahtjeve za ISMS

Definira “što” organizacija treba učiniti da bi zaštitila svoje informacije

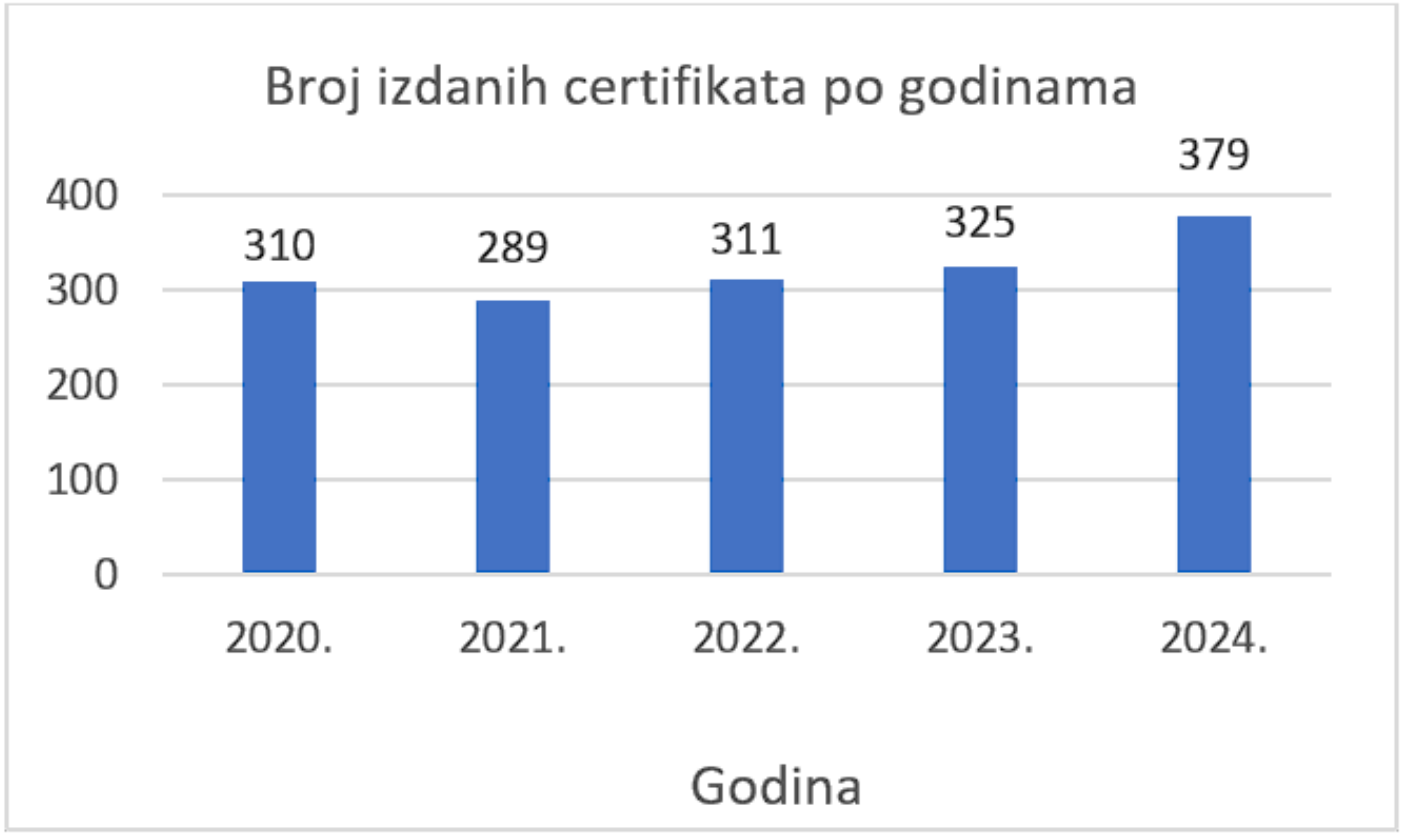
ISO/IEC 27002:2022

Sadrži smjernice i najbolje prakse za implementaciju kontrola informacijske sigurnosti

Definira „kako” primijeniti sigurnosne kontrole

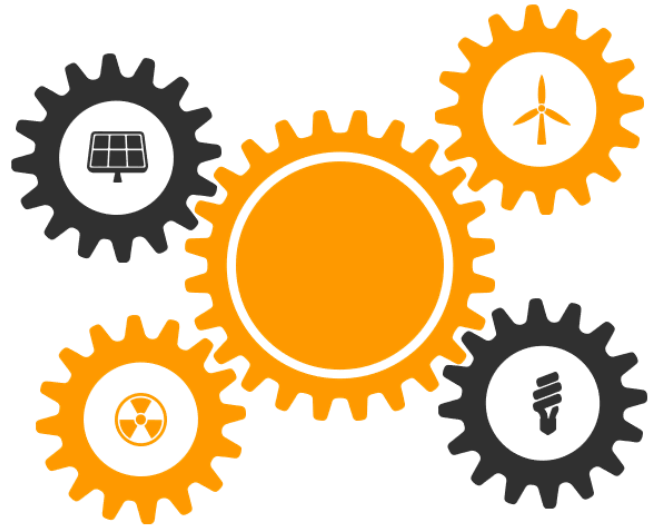


KRETANJE BROJA CERTIFIKATA ISO/IEC 27001 U RH



IMPLEMENTACIJA ISO/IEC 27001 U PODSUSTAVE PAMETNOG GRADA

- Sustav ISMS se ne uvodi i ne certificira na razini cjelokupnog grada
- Postupak se primjenjuje na pojedine odjele ili organizacijske jedinice koje upravljaju kritičnom infrastrukturom i informacijskim sustavima.
- Svaka od tih jedinica – bilo da se radi o odjelu za upravljanje prometom, energetskoj infrastrukturi, javnim digitalnim servisima ili IT odjelu – implementira sustav upravljanja informacijskom sigurnošću (ISMS) i stječe zasebni certifikat ISO/IEC 27001.



PREGLED POTENCIJALNIH ORGANIZACIJSKIH JEDINICA PAMETNOG GRADA

Primjer organizacijske jedinice	Opis djelatnosti	Područje primjene norme ISO/IEC 27001	Fokus ISO/IEC 27001
Promet i mobilnost (Smart Mobility)	Sustavi za upravljanje prometom, pametni semafori, prometni senzori, parkirališne platforme, električni punjači, javni prijevoz (automatsko praćenje i naplata)	Sustav nadzora prometa i prometnih podataka Elektroničke karte i sustavi naplate Mobilne aplikacije za građane koje prikupljaju lokacijske podatke	Zaštita podataka o lokaciji, sigurnost komunikacije između uređaja, kontrola pristupa administratora i servisa
Vodovod i sl. energetski sustavi (Smart Utilities)	IoT senzori za vodu, plin, električnu energiju, pametni brojila, sustavi praćenja potrošnje.	Centralni sustav nadzora i upravljanja distribucijom energije IoT platforma koja prikuplja i analizira potrošnju građana	Zaštita integriteta i dostupnosti podataka, sprječavanje neautoriziranog pristupa i manipulacije brojila, sigurnost u prijenosu podataka
Zdravstvo i socijalni sustavi (Smart Health & Social Services)	Elektronički zdravstveni kartoni, sustavi za praćenje pacijenata, socijalne usluge i e-usluge građanima	E zdravstvo (eHealth) platforma Sustav za terminiranje i upravljanje podacima pacijenata	Povjerljivost i integritet zdravstvenih podataka, kontrola pristupa, enkripcija komunikacije, audit aktivnosti
Obrazovanje (Smart Education)	Digitalne platforme za škole i fakultete, e-učenje, administracija učenika i nastavnog kadra.	Platforme za praćenje prisutnosti i ocjena učenika Sustavi e-učenja i online pristupa materijalima za učenje	Zaštita osobnih podataka učenika, sigurnost lozinki i autentifikacije, zaštita od krađe podataka i cyber prijetnji
E-usluge grada i administracija (Smart Governance)	Platforme za izdavanje dokumenata, prijava problema u gradu, plaćanje komunalnih naknada, elektronički obrasci i aplikacije	Portal e-uprave Sustav registracije i autentifikacije građana	Povjerljivost i integritet podataka građana, autentifikacija, dostupnost servisa, sigurnost baze podataka

ZAHTJEVI ISO/IEC 27001:2022 I KONTROLE ISO/IEC 27002:2022

➢ Primjeri najvažnijih zahtjeva iz norme ISO/IEC 27001 te sigurnosnih kontrola koje bi bile primjenjive za sve ranije pretpostavljene jedinice pametnog grada:

Najvažniji zahtjevi norme ISO/IEC 27001	Opis zahtjeva i primjena u organizacijskim jedinicama pametnog grada
Procjena rizika informacijske sigurnosti (zahtjev 6.1.2)	Organizacija mora identificirati, procijeniti i klasificirati rizike informacijske sigurnosti. Primjena: svi gradski odjeli imaju rizike za informacije koje posjeduju, IoT uređajima i IT sustavima (promet, energija, komunalije…).
Tretiranje rizika informacijske sigurnosti (zahtjev 6.1.3)	Organizacija mora odabrati i primijeniti odgovarajuće sigurnosne kontrole te izraditi Statement of Applicability (SoA). Primjena: gradska uprava centralno određuje koje kontrole vrijede za sve odjele i sustave pametnog grada.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

- Norma ISO/IEC 27001 od organizacija zahtjeva definiranje i primjenu postupka procjene rizika informacijske sigurnosti prema unaprijed definiranoj metodologiji te korištenje izlaza procjene za donošenje odluka o konkretnim zaštitnim mjerama koje će organizacija primijeniti u cilju minimiziranja prepoznatih rizika.
- Početni korak procjene rizika je definiranje kriterija prihvatljivosti (kvantificiranje razine na kojoj se neki rizik smatra dovoljno malim da se prihvati bez dodatnih mjera) te definiranje metodologije provedbe procjene rizika (definiranje procesa ocjene rizika).
- Prema zahtjevu norme ISO/IEC 27001 6.1.2 d) procjena ukupnog rizika se temelji na procjeni potencijalne posljedice koja bi nastala ako bi se rizik ostvario te procjeni realne vjerojatnosti pojave rizika. Uobičajeni pristup uključuje korištenje matrice rizika od tri ili pet stupnjeva vjerojatnosti i ukupnog rizika.

	Vjerojatnost incidenta scenarija	Vrlo mala	Mala	Srednja	Visoka	Vrlo visoka
Utjecaj posljedica	Vrlo mala	3	4	5	6	7
	Mala	4	5	6	7	8
	Srednja	5	6	7	8	9
	Visoka	6	7	8	9	10
	Vrlo visoka	7	8	9	10	11

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

- Sljedeći korak procjene rizika je identifikacija realnih rizika povezanih s gubitkom povjerljivosti, cjelovitosti i dostupnosti informacija unutar opsega sustava upravljanja informacijskom sigurnošću, identifikacija vlasnika rizika te provedba vrednovanja rizika u skladu s ranije definiranom metodologijom.
- Rezultat provedene analize je pregled identificiranih rizika koje će organizacija, u skladu s utvrđenom razinom ozbiljnosti svakog rizika, tretirati korištenjem neke od kontrola iz norme ISO/IEC 27001 i ISO/IEC 27002.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

Opis rizika	Vjerojatnost	Utjecaj	Razina rizika	Predložene mjere (kontrole)
Neovlašten pristup sustavu zbog slabih lozinki	Visoka	Visok	Kritičan	Uvođenje višefaktorske autentifikacije, politika složenih lozinki
Ucjenjivački napad	Srednja	Vrlo visok	Kritičan	Redoviti backup, antivirus, segmentacija mreže, edukacija korisnika
Opis rizika	**Vjerojatnost**	**Utjecaj**	**Razina rizika**	**Predložene mjere (kontrole)**
Napad lažnim predstavljanjem	Visoka	Visok	Kritičan	Edukacija korisnika, email filteri, simulacije phishinga
Nezakrpani sigurnosni propusti u softveru	Srednja	Visok	Visok	Redovito ažuriranje softvera, patch management politika
Pogrešna konfiguracija mrežnih uređaja	Srednja	Visok	Visok	Redoviti sigurnosni auditi, segmentacija mreže, kontrola konfiguracija
Nedostatak sigurnosnih kopija (backup)	Srednja	Visok	Visok	Automatizirani backup sustav, redovito testiranje povrata podataka

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

- Zahtjev 6.1.3 norme ISO/IEC 27001 zahtijeva definiranje procesa obrade rizika informacijske sigurnosti kojim organizacija odabire odgovarajuće strategije upravljanja rizicima te implementira sigurnosne kontrole kako bi smanjila identificirane prijetnje na prihvatljivu razinu.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

<table>
<tr><th>Opis rizika</th><th>Tretiranje rizika</th></tr>
<tr><td>Neovlašten pristup sustavu zbog slabih lozinki</td><td>Neovlašten pristup sustavu za upravljanje pametnom rasvjetom.</td></tr>
<tr><td>Odabir načina postupanja s rizikom</td><td>Smanjivanje rizika</td></tr>
<tr><td>Primjenjive kontrole iz norme ISO/IEC 27001</td><td>- višefaktorska autentifikacija za administratore,
- segmentacija mreže za IoT uređaje,
- zapisivanje i praćenje pristupa (logiranje).</td></tr>
<tr><td>Izjava o primjenjivosti (SoA)</td><td>
<table>
<tr><th>Kontrola</th><th>Primjenjiva</th><th>Obrazloženje</th><th>Status</th></tr>
<tr><td>Upravljanje pristupom</td><td>Da</td><td>Sprječavanje neovlaštenog pristupa sustavu</td><td>U implementaciji</td></tr>
<tr><td>Upravljanje identitetima</td><td>Da</td><td>Potrebno za MFA</td><td>Implementirano</td></tr>
<tr><td>Kriptografija</td><td>Da</td><td>Za zaštitu komunikacije uređaja</td><td>Implementirano</td></tr>
</table>
</td></tr>
<tr><td>Plan obrade rizika</td><td>
<table>
<tr><th colspan="4">Plan obrade rizika</th></tr>
<tr><th>Rizik</th><th>Kontrola</th><th>Odgovorna osoba</th><th>Rok</th></tr>
<tr><td>Neovlašten pristup IoT sustavu</td><td>MFA + segmentacija mreže</td><td>IT voditelj</td><td>3 mjeseca</td></tr>
</table>
</td></tr>
<tr><td>Odobrenje rezidualnog rizika</td><td>Direktor odobrava da je preostali rizik prihvatljiv nakon implementacije kontrola.</td></tr>
</table>

ZAHTJEVI ISO/IEC 27001:2022 I KONTROLE ISO/IEC 27002:2022

- Pregled karakterističnih sigurnosnih kontrola univerzalno primjenjivih na sve organizacijske jedinice pametnog grada iz dodatka A norme ISO/IEC 27001 te ISO/IEC 27002

Kontrola fizičkog pristupa (kontrola 7.2)	Osigurava da samo ovlaštene osobe mogu ući u podatkovne centre, kontrolne sobe i tehničke prostorije. Primjena: kontrolirani pristup podatkovnim centrima i serverima grada ili centrima pojedinih organizacijskih jedinica pametnog grada.
Kriptografske kontrole (kontrola 8.5)	Zaštita informacija korištenjem kriptografskih metoda (enkripcija, digitalni potpisi). Primjena: kriptiranje osobnih podataka građana kojima sustavi raspolažu, sigurni prijenosi podataka IoT uređaja i IT sustava, zaštita povjerljivih dokumenata itd.
Sigurnost mreže, mrežnih usluga i segregacija mreža (kontrole 8.20, 8.21, 8.22)	Kontrola sigurnosti mreže zahtijeva zaštitu i upravljanje mrežama kako bi se spriječio neovlašteni pristup i kompromitacija sustava; Kontrola sigurnosti mrežnih usluga osigurava sigurnost i pouzdanost mrežnih usluga kroz autentifikaciju, nadzor i evidenciju aktivnosti; Kontrola segregacije mreža osigurava odvajanje mrežnih segmenata i sustava kako bi se spriječilo lateralno širenje napada te ograničio pristup između različitih dijelova sustava. Primjena: IoT senzori za kvalitetu zraka šalju podatke samo u analitički sustav, a administratori pristupaju konfiguraciji putem VPN-a i višefaktorske autentifikacije. Javni Wi-Fi u parkovima je izoliran od mreže kritične infrastrukture, a pametna rasvjeta i nadzor kamera imaju zasebne, odvojene mrežne zone s kontroliranim pristupom.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

Kontrola 7.2; Kontrola fizičkog pristupa

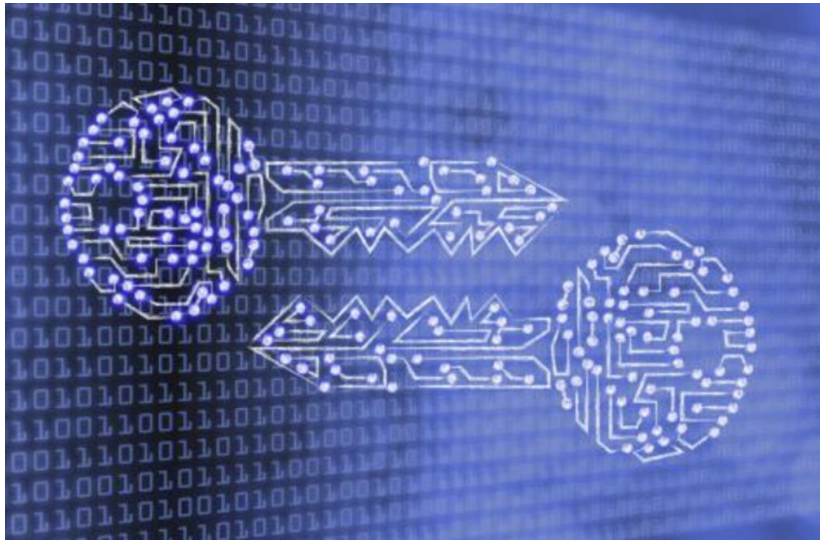
- Kontrola 7.2 norme ISO/IEC 27002 zahtijeva definiranje jasnih mjera za fizičku zaštitu prostorija i objekata u kojima se nalaze informacijski sustavi, uređaji te sami podaci.
- Cilj: spriječiti neovlašteni pristup, krađu, oštećenje ili neautorizirane intervencije.
- Provedbeno: definiranje pravila pristupa, dodjela odgovornosti, vođenje evidencije ulazaka i izlazaka, nadzor prostora te redovite provjere učinkovitosti tih mjera.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

Kontrola 8.5; Kriptografske kontrole

- Organizacija mora osigurati pravilnu i učinkovitu upotrebu kriptografije za zaštitu povjerljivosti, autentičnosti i integriteta informacija, a u skladu s poslovnim i zahtjevima informacijske sigurnosti te uzimajući u obzir zakonske, regulatorne i ugovorne obveze vezane uz kriptografiju.

- U praksi, kontrola uključuje definiranje politike i pravila za kriptografiju: definiranje kada i gdje se koristi enkripcija - npr. za prijenos podataka e-mailom, pohranu osjetljivih podataka, zaštitu lozinki, digitalne potpise, definiranje standarda algoritama - npr. AES-256, RSA-2048, SHA-256, definiranje duljine ključeva, načine generiranja i trajanje valjanosti, upravljanje kriptografskim ključevima i sl.



PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

Kontrole 8.20, 8.21, 8.22; Sigurnost mreže, mrežnih usluga i segregacija mreže

- Upravljanje mrežnom sigurnošću je jedna od ključnih IT kontrola u okviru sustava upravljanja informacijskom sigurnošću
- Kontrola zahtijeva da mreže i mrežni uređaji budu pravilno zaštićeni i upravljani kako bi se spriječilo neovlašteno korištenje, kompromitacija ili širenje eventualnih napada
- To uključuje definiranje tko je odgovoran za upravljanje mrežom, pravila pristupa i standarde konfiguracije uređaja, kao i stalni nadzor mrežnog prometa
- U praksi, primjer u pametnom gradu može biti situacija u kojoj svi IoT senzori za kvalitetu zraka šalju podatke u centralni analitički sustav preko zaštićenih kanala, dok pristup njihovoj konfiguraciji imaju samo ovlašteni tehničari putem VPN-a i višefaktorske autentifikacije.

PRIMJER ISPUNJENJA ZAHTJEVA NORME ISO/IEC 27001

- Svi servisi moraju biti konfigurirani prema sigurnosnim standardima, uključujući šifriranje komunikacije, autentifikaciju korisnika i vođenje evidencije aktivnosti.

- Primjer implementacije je VPN pristup za administratore nadzornih kamera s višefaktorskom autentifikacijom, dok građani i operateri e-uprave pristupaju svojim podacima preko kontroliranog portala s logiranjem aktivnosti i ograničenim pravima.

- Obavezna je segmentacija mreže, odnosno odvajanje različitih sustava i korisnika u zasebne zone, kako bi se smanjio rizik od širenja napada ili neovlaštenog pristupa.

- IoT senzori i prometni senzori smješteni u odvojene VLAN-ove koji šalju podatke isključivo u analitički sustav, bez pristupa kritičnim kontrolnim sustavima. Javni Wi-Fi u parkovima izoliran je od mreža kritične infrastrukture, s pristupom samo internetu i ograničenom komunikacijom s drugim segmentima. Sustavi video nadzora također su u zasebnom segmentu, gdje administratori mogu pristupati isključivo kamerama pod svojom odgovornošću, a sustav bilježi sve pristupe i aktivnosti.

ZAKLJUČAK

ISO/IEC 27001

- Povećava razinu sigurnosti informacija i smanjuje rizik od sigurnosnih incidenata
- Pomaže u usklađivanju s pravnim i regulatornim zahtjevima, poput zaštite osobnih podataka
- Jača povjerenje korisnika, partnera i investitora

Koncept pametnog grada

- Važan element suvremenog urbanog razvoja
- Integracijom tehnologije, podataka i inovativnih modela upravljanja moguće je povećati učinkovitost gradskih sustava, ali i unaprijediti kvalitetu života građana te održivost urbanih sredina

Kontinuirani izazov

- Implementacija zahtijeva koordinaciju svih zainteresiranih strana, kao i moguću prilagodbu poslovnih procesa

Budućnost

- Daljnji razvoj pametnih gradova, kao i povećanje broja digitalnih sustava koji će biti dijelovi gradskih infrastruktura


HVALA
NA
POZORNOSTI