



PRAVILA KORIŠTENJA SUSTAVA UMJETNE INTELIGENCIJE ZA NADZOR MIKROKLIMATSKIH UVJETA U SERVER SOBI

Naziv ustanove: SPECIJALNA BOLNICA ZA PLUĆNE BOLESTI

Organizacijska jedinica: IT odjel

Verzija dokumenta: 1.4

Datum donošenja: 01.01.2025.

1. Svrha dokumenta

Ovim dokumentom uređuju se pravila korištenja sustava umjetne inteligencije koji se koristi u ustanovi isključivo za nadzor mikroklimatskih uvjeta u server sobi.

Svrha sustava je praćenje tehničkih i okolišnih parametara koji mogu utjecati na siguran i stabilan rad serverske, mrežne i komunikacijske infrastrukture ustanove.

Sustav se koristi kao pomoćni tehnički alat za rano upozoravanje na moguće nepravilnosti, odstupanja ili rizike povezane s mikroklimatskim uvjetima u server sobi.

2. Opis sustava

Sustav za nadzor mikroklimatskih uvjeta sastoji se od senzorskih uređaja, aplikacijskog sučelja, baze podataka i programskog modula za analizu prikupljenih podataka.

Sustav prati sljedeće parametre:

- temperaturu,
- relativnu vlagu zraka,
- eventualne dodatne okolišne ili tehničke parametre ako su omogućeni senzorima,
- dostupnost senzorskih uređaja,
- promjene i odstupanja od zadanih pragova.

Programski modul koristi algoritamsku analizu i elemente umjetne inteligencije za prepoznavanje neuobičajenih promjena, trendova ili odstupanja u izmjenjenim vrijednostima. Sustav može generirati upozorenja odgovornim osobama u slučaju prekoračenja zadanih vrijednosti ili pojave uvjeta koji mogu predstavljati rizik za rad informacijske infrastrukture.



3. Područje primjene

Ova pravila primjenjuju se na korištenje sustava za nadzor mikroklimatskih uvjeta u server sobi ustanove.

Pravila se odnose na:

- administratore sustava,
- djelatnike informatičke službe,
- ovlaštene osobe zadužene za održavanje server sobe,
- osobe koje imaju pristup prikazu, izvješćima ili obavijestima iz sustava.

Sustav se ne koristi u drugim poslovnim procesima ustanove, osim u svrhu tehničkog nadzora mikroklimatskih uvjeta i zaštite informacijske infrastrukture.

4. Dopuštena svrha korištenja

Sustav se smije koristiti isključivo za:

1. nadzor temperature i vlage u server sobi,
2. praćenje stabilnosti mikroklimatskih uvjeta,
3. rano upozoravanje na moguće tehničke rizike,
4. evidenciju izmjerenih vrijednosti,
5. izradu tehničkih izvješća o stanju mikroklimе,
6. pomoć pri održavanju serverske i mrežne infrastrukture,
7. smanjenje rizika od prekida rada informacijskih sustava.

Sustav se ne smije koristiti za svrhe koje nisu povezane s tehničkim nadzorom server sobe.

5. Ograničenja korištenja sustava

Sustav se ne koristi za:

- donošenje odluka o pravima, obvezama ili interesima fizičkih osoba,
- automatizirano odlučivanje o pacijentima, zaposlenicima ili korisnicima usluga ustanove,
- profiliranje fizičkih osoba,
- obradu zdravstvenih podataka,
- obradu osobnih podataka pacijenata,
- obradu osobnih podataka zaposlenika u svrhu procjene rada ili ponašanja,



- biometrijsku identifikaciju,
- nadzor ponašanja osoba,
- sigurnosno profiliranje osoba,
- donošenje upravnih, radnopravnih, medicinskih ili financijskih odluka.

Sustav nema ovlast samostalno donositi odluke koje bi imale pravne, organizacijske, medicinske ili druge posljedice za fizičke osobe.

6. Vrste podataka koje sustav obrađuje

Sustav obrađuje tehničke i okolišne podatke, kao što su:

- temperatura prostora,
- relativna vlaga zraka,
- vrijeme mjerenja,
- identifikator senzorskog uređaja,
- status uređaja,
- stanje komunikacije uređaja,
- tehničke obavijesti i alarmi,
- povijesni zapisi mjerenja.

Sustav ne obrađuje osobne podatke pacijenata, korisnika zdravstvenih usluga ili drugih fizičkih osoba.

Ako se u sustavu evidentiraju korisnička imena administratora ili tehničkog osoblja radi pristupa sustavu, takvi se podaci koriste isključivo za kontrolu pristupa, sigurnosnu evidenciju i revizijski trag.

7. Ljudski nadzor

Sustav služi kao pomoćni alat i ne zamjenjuje ljudski nadzor. Svako upozorenje koje sustav generira provjerava ovlaštena osoba informatičke službe ili druga odgovorna osoba ustanove.

Konačnu procjenu stanja, odluku o intervenciji i poduzimanje tehničkih mjera donosi ovlaštena osoba.

Sustav ne provodi samostalne fizičke radnje na infrastrukturi, osim ako je posebno konfiguriran za slanje obavijesti ili aktiviranje tehničkih alarma.



8. Ovlaštenja i pristup sustavu

Pristup sustavu imaju samo ovlaštene osobe. Korisnička prava dodjeljuju se prema načelu najmanjih potrebnih ovlasti.

Pristup može uključivati sljedeće razine:

1. Pregled podataka – pregled trenutnih i povijesnih vrijednosti.
2. Administracija pragova – uređivanje dopuštenih granica temperature, vlage i drugih parametara.
3. Administracija sustava – upravljanje uređajima, korisnicima i tehničkim postavkama.
4. Izvješćivanje – izrada i izvoz izvješća.

Zabranjeno je dijeljenje korisničkih računa, lozinki ili pristupnih podataka.

9. Pravila za postavljanje alarmnih pragova

Alarmni pragovi postavljaju se prema tehničkim zahtjevima serverske, mrežne i komunikacijske opreme te prema internim pravilima održavanja server sobe.

Primjeri pragova mogu uključivati:

- upozorenje kod povišene temperature,
- kritični alarm kod značajnog prekoračenja temperature,
- upozorenje kod previsoke ili preniske relativne vlage,
- alarm u slučaju prekida komunikacije sa senzorom,
- alarm u slučaju nedostupnosti uređaja.

Promjene alarmnih pragova smiju provoditi samo ovlaštene osobe.

Svaka značajna promjena pragova mora biti opravdana tehničkom potrebom.

10. Obavijesti i alarmi

Sustav može slati obavijesti putem aplikacijskog sučelja, elektroničke pošte, SMS-a, push obavijesti ili drugog tehničkog kanala ako je takav način obavješćivanja omogućen.

Obavijesti služe za pravovremeno informiranje odgovornih osoba o mogućem tehničkom riziku.

Primanje obavijesti ne znači da je sustav donio konačnu odluku o stanju infrastrukture, već da je potrebno izvršiti provjeru.

Ovlaštena osoba nakon primitka obavijesti provjerava stanje i po potrebi poduzima odgovarajuće tehničke mjere.



11. Evidencija i revizijski trag

Sustav može voditi evidenciju o:

- izmjerenim vrijednostima,
- generiranim alarmima,
- vremenu nastanka alarma,
- statusu senzorskih uređaja,
- prijavama korisnika,
- administrativnim promjenama,
- promjenama pragova,
- tehničkim intervencijama ako se evidentiraju u sustavu.

Revizijski trag koristi se za sigurnosnu provjeru, održavanje sustava, analizu incidenata i dokazivanje pravilnog rada sustava.

12. Postupanje u slučaju alarma

U slučaju alarma ili upozorenja, ovlaštena osoba postupa prema sljedećim koracima:

1. provjerava prikaz u sustavu,
2. provjerava je li alarm posljedica stvarnog odstupanja ili tehničke greške senzora,
3. po potrebi fizički provjerava stanje server sobe,
4. provjerava rad klimatizacije, napajanja i mrežne infrastrukture,
5. obavještava nadležne osobe ako postoji rizik za rad informacijskih sustava,
6. evidentira poduzete mjere ako je to potrebno,
7. prati normalizaciju vrijednosti nakon intervencije.

Ako se utvrdi ozbiljan rizik za rad server sobe, postupa se prema internim pravilima za upravljanje incidentima i kontinuitet poslovanja.

13. Sigurnost sustava

Sustav mora biti zaštićen odgovarajućim tehničkim i organizacijskim mjerama.

Mjere uključuju:

- ograničen pristup ovlaštenim korisnicima,
- korištenje lozinki ili drugog mehanizma autentifikacije,



- redovito ažuriranje sustava,
- zaštitu komunikacijskih kanala gdje je primjenjivo,
- sigurnosno kopiranje podataka ako je sustav konfiguriran za dugoročnu pohranu,
- kontrolu pristupa administracijskim funkcijama,
- zaštitu od neovlaštenih promjena alarmnih pragova.

14. Točnost i pouzdanost sustava

Ovlaštene osobe dužne su povremeno provjeravati ispravnost senzora i vjerodostojnost prikazanih vrijednosti.

Ako postoji sumnja u neispravnost senzora, pogrešno očitavanje ili tehnički kvar, podaci iz sustava ne smiju se koristiti kao jedina osnova za procjenu stanja.

U slučaju sumnje u ispravnost sustava potrebno je izvršiti tehničku provjeru, servisiranje ili zamjenu opreme.

15. Čuvanje podataka

Podaci se čuvaju u razdoblju koje je potrebno za tehničko praćenje, analizu trendova, održavanje sustava i dokazivanje postupanja u slučaju incidenata.

Rok čuvanja podataka određuje se internim pravilima ustanove i tehničkim mogućnostima sustava.

Podaci koji više nisu potrebni mogu se arhivirati ili brisati sukladno internim pravilima ustanove.

16. Zabranjene radnje

Zabranjeno je:

- koristiti sustav za nadzor osoba,
- unositi osobne ili zdravstvene podatke u sustav,
- mijenjati alarmne pragove bez ovlaštenja,
- isključivati alarme bez opravdanog razloga,
- dijeliti pristupne podatke,
- neovlašteno izvoziti podatke,
- koristiti podatke iz sustava za svrhe koje nisu povezane s nadzorom server sobe,



- onemogućavati rad sustava bez odobrenja odgovorne osobe.

17. Odgovornosti

Za pravilno korištenje sustava odgovorna je informatički odjel ustanove.

Odgovorna osoba za sustav dužna je:

- osigurati pravilnu konfiguraciju sustava,
- nadzirati rad sustava,
- provjeravati alarme i upozorenja,
- osigurati da pristup imaju samo ovlaštene osobe,
- voditi računa o sigurnosti sustava,
- predlagati poboljšanja sustava,
- prijaviti ozbiljne tehničke incidente nadležnim osobama.

Korisnici sustava dužni su koristiti sustav savjesno, u skladu s ovim pravilima i isključivo u dopuštene svrhe.

18. Postupanje u slučaju incidenta

Incidentom se smatra svaki događaj koji može utjecati na pouzdanost, dostupnost ili sigurnost sustava, uključujući:

- neovlašten pristup sustavu,
- gubitak podataka,
- netočne ili nelogične vrijednosti mjerenja,
- prekid rada senzora,
- prekid komunikacije,
- neovlaštenu promjenu pragova,
- nepravilno generiranje ili izostanak alarma.

U slučaju incidenta ovlaštena osoba mora poduzeti razumne mjere za ograničavanje posljedica, provjeru uzroka i obnovu normalnog rada sustava.

Ako incident može utjecati na rad drugih informacijskih sustava ustanove, o tome se obavještavaju nadležne osobe prema internim procedurama ustanove.



19. Transparentnost i dokumentiranje

Ustanova vodi osnovnu dokumentaciju o korištenju sustava, uključujući:

- opis svrhe sustava,
- opis vrste podataka koji se obrađuju,
- opis funkcionalnosti sustava,
- popis ovlaštenih osoba ili uloga,
- pravila korištenja,
- evidenciju značajnih promjena sustava, ako je primjenjivo.

Na zahtjev nadležnih tijela, ustanova može dostaviti relevantne informacije o sustavu u skladu s važećim propisima i internim pravilima.

20. Periodična provjera i izmjene pravila

Ova pravila preispituju se prema potrebi, a najmanje u slučaju:

- značajne promjene funkcionalnosti sustava,
- proširenja sustava na druge prostore ili procese,
- uvođenja novih vrsta senzora,
- promjene pravnog ili regulatornog okvira,
- sigurnosnog incidenta,
- utvrđene potrebe za poboljšanjem kontrole korištenja.

Izmjene pravila odobrava odgovorna osoba ustanove.

21. Završne odredbe

Ova pravila stupaju na snagu danom donošenja.

Svi korisnici koji imaju pristup sustavu dužni su pridržavati se ovih pravila.

Sustav umjetne inteligencije opisan ovim pravilima koristi se isključivo kao tehnički pomoćni alat za nadzor mikroklimatskih uvjeta u server sobi i ne koristi se za odlučivanje o fizičkim osobama, pacijentima, zaposlenicima ili korisnicima usluga ustanove.

Specijalna bolnica za plućne bolesti
ravnateljica
prim.dr.sc. Ana Šoštarić Zadro, dr.med.

