VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

VARNOSTNA ANALIZA LOKALNEGA IN OBLAČNEGA SHRANJEVANJA PODATKOV PRI CELIČNIH TERAPIJAH

Kandidat: Jalen Arko

Vrsta študija: Študent izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Matic Gobec

Lektorica: Marjeta Vozlič, prof. slov. jez.

Maribor, 2026

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Jalen Arko sem avtor diplomskega dela z naslovom Varnostna analiza lokalnega in oblačnega shranjevanja podatkov pri celičnih terapijah, ki sem ga napisal pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel/a, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Ljubljana, februar 2026 Podpis študenta:

ZAHVALA

Ob zaključku diplomskega dela se iskreno zahvaljujem vsem, ki so mi na različne načine pomagali in me podpirali v času študija ter pri pripravi tega dela. Najprej se zahvaljujem svoji družini, ki mi je skozi celotno obdobje izobraževanja stala ob strani, mi nudila podporo ter razumevanje pri usklajevanju študijskih in osebnih obveznosti. Njihova spodbuda je pomembno prispevala k moji vztrajnosti in uspešnemu zaključku študija.

Posebno zahvalo namenjam svoji partnerki Tanji za potrpežljivost, razumevanje in nenehno podporo v času pisanja diplomskega dela. Njena spodbuda in pripravljenost prisluhniti sta mi bili v veliko pomoč pri soočanju z izzivi, povezanimi s študijem in delom.

Zahvaljujem se tudi podjetju, ki mi je omogočilo opravljanje praktičnega dela ter mi dalo priložnost za zaposlitev. S tem sem lahko pridobil dragocene praktične izkušnje in poglobljeno razumevanje obravnavane tematike. Delo v realnem delovnem okolju mi je omogočilo, da sem teoretično znanje povezal s prakso in ga uporabil pri pripravi diplomskega dela.

Iskrena zahvala gre tudi sodelavcem, ki so bili vedno pripravljeni deliti svoje znanje, izkušnje in strokovne nasvete. Njihova odprtost in strokovna pomoč so pomembno prispevale k razumevanju delovanja informacijskih sistemov v raziskovalnem okolju.

Na koncu se zahvaljujem tudi vsem predavateljem in mentorjem, ki so me skozi študij usmerjali, mi posredovali znanje ter prispevali k mojemu strokovnemu in osebnemu razvoju. Vsem navedenim se iskreno zahvaljujem za podporo in pomoč pri moji izobraževalni poti.

POVZETEK

Diplomsko delo obravnava upravljanje, organizacijo in varnost shranjevanja podatkov v biotehnološkem raziskovalnem okolju, kjer imajo podatki visoko raziskovalno, razvojno in poslovno vrednost. Osrednji poudarek naloge je na primerjavi lokalne infrastrukture in oblačnih storitev ter na analizi njune vloge pri zagotavljanju varnosti podatkov, preglednosti dela in učinkovitosti delovnih procesov. Namen naloge je bil proučiti obstoječe prakse shranjevanja podatkov v podjetju, identificirati morebitna tveganja in ranljivosti ter na tej podlagi oblikovati realne in izvedljive predloge izboljšav.

V teoretičnem delu naloge so predstavljeni osnovni pojmi informacijske varnosti, značilnosti lokalnega shranjevanja podatkov in oblačnih storitev ter splošna tveganja, povezana z upravljanjem informacijskih sistemov. Poseben poudarek je namenjen vlogi človeškega faktorja in organizacijskih postopkov, saj ti pogosto predstavljajo pomemben vir varnostnih ranljivosti. Teoretična izhodišča služijo kot podlaga za razumevanje praktičnega dela naloge.

V empiričnem delu je analizirano dejansko stanje v podjetju, kjer se lokalna infrastruktura uporablja za shranjevanje raziskovalnih podatkov, eksperimentalnih rezultatov, analiz in druge občutljive dokumentacije. Oblačne storitve se uporabljajo predvsem kot podporno okolje za komunikacijo, organizacijo dela in načrtovanje aktivnosti. Analiza je pokazala, da je takšna razmejitev zavestna in prilagojena naravi raziskovalnega dela.

Rezultati analize kažejo, da je obstoječi sistem tehnično stabilen in ustrezno zaščiten, pri čemer večina zaznanih tveganj in ranljivosti ne izhaja iz tehničnih pomanjkljivosti, temveč iz organizacijskih postopkov in načina uporabe sistemov. Med pomembnejšimi izzivi so upravljanje dostopnih pravic, doslednost pri shranjevanju podatkov ter neformalni načini uporabe oblačnih orodij. Na podlagi ugotovitev so bili oblikovani predlogi varnostnih nadgradenj, optimizacije obstoječega načina dela ter izboljšav na področju varnostnih kopij in upravljanja dostopov.

Diplomsko delo ugotavlja, da kombinacija lokalnega in oblačnega shranjevanja podatkov omogoča uravnotežen pristop med varnostjo in učinkovitostjo dela. Ključno vlogo pri tem ima jasno določanje vlog posameznih sistemov ter dosledno upravljanje dostopov in podatkov.

Ključne besede: *informacijska varnost, lokalno shranjevanje podatkov, oblačne storitve, varnost podatkov, upravljanje dostopov, biotehnološko raziskovalno okolje*

ABSTRACT

Security Analysis of Local and Cloud Data Storage in Cellular Therapy Research

This diploma thesis examines the management, organization, and security of data storage in a biotechnological research environment, where data represent significant scientific, developmental, and business value. The main focus of the thesis is a comparison between local infrastructure and cloud-based services, with an emphasis on their roles in ensuring data security, work efficiency, and organizational transparency. The objective of the thesis was to analyze existing data storage practices within the company, identify potential risks and vulnerabilities, and propose realistic and feasible improvements.

The theoretical part of the thesis introduces fundamental concepts of information security, characteristics of local data storage, and cloud services, as well as general risks associated with information system management. Particular attention is given to organizational factors and the human element, as these often represent a critical source of security vulnerabilities. The theoretical framework serves as a foundation for understanding the practical analysis.

The empirical part analyzes the actual data management practices within the company. Local infrastructure is used for storing research data, experimental results, analyses, and other sensitive documentation, while cloud services are primarily employed to support communication, task organization, and coordination of work activities. The analysis shows that this separation is intentional and aligned with the security requirements of a research-oriented environment.

The results indicate that the existing system is technically stable and adequately protected. Most identified risks and vulnerabilities are not technical in nature but are instead related to organizational procedures and user behavior. Based on these findings, the thesis proposes security enhancements, optimization of existing workflows, and improvements in backup management and access control. The study concludes that a combined use of local and cloud-based storage provides a balanced approach between security and operational efficiency, provided that system roles and access rights are clearly defined and consistently managed.

Keywords: *Information security, local data storage, cloud services, data management, access control, data backups, biotechnological research environment*

KAZALO VSEBINE

1. UVOD 9

1.1 Opis področja in kontekst raziskave 9
1.3 Pomen podatkov v procesih celičnih terapij 10
1.4 Namen, cilji in raziskovalna vprašanja 10
1.5 Metodologija raziskovalnega dela 11

2. TEORETIČNA IZHODIŠČA 12

2.1 Podatkovni sistemi v biotehnologiji 12
2.1.1 Vrste podatkov v laboratorijskem okolju 12
2.1.2 Občutljivost in kritičnost bioloških podatkov 12
2.1.3 Zahteve za sledljivost in arhiviranje podatkov 13
2.2 Lokalna IT-infrastruktura 14
2.2.1 Lokalni strežniki – arhitektura in delovanje 14
2.2.2 Sistemi NAS, RAID in redundanca 15
2.2.3 Prednosti in slabosti lokalne infrastrukture 18
2.2.4 Varnostni mehanizmi lokalnih sistemov 18
2.3 Oblačne storitve 19
2.3.1 Osnovni modeli oblačnih storitev (IaaS, PaaS, SaaS) 19
2.3.2 Prednosti in slabosti oblačnih rešitev 20
2.3.3 Varnostni mehanizmi v oblaku 21
2.3.4 Tipična uporaba oblaka v podjetjih 22
2.4 Primerjava lokalnega in oblačnega shranjevanja 22
2.4.1 Razlike v nadzoru in arhitekturi 22
2.4.2 Razlike v stroških, dostopu in uporabi 23
2.4.3 Analiza tveganj 24
2.5 Kibernetska varnost 25
2.5.1 Vrste groženj 26
2.5.2 Preventivni in korektivni ukrepi 27
2.5.3 Vloga avtentikacije, šifriranja in segmentacije omrežij 28
2.5.4 Sodobni trendi v kibernetski varnosti 30
3. REGULATIVNA IZHODIŠČA 32
3.1 GDPR in varovanje osebnih podatkov 32
3.2 ISO/IEC 27001 in informacijska varnost 33
3.3 Zahteve za ravnanje z laboratorijskimi podatki 33
3.4 Regulativa povezana z delom z biološkimi materiali 34

4. OPIS PODJETJA IN KONTEKSTA DELA 36

4.1 Področje dejavnosti podjetja 36
4.2 Značilnosti laboratorijskih postopkov 36
4.3 Vrste podatkov, ki nastajajo pri delu 37
4.4 Obstoječa IT-infrastruktura 37
4.5 Trenutni način shranjevanja podatkov 39

5. ANALIZA LOKALNEGA SHRANJEVANJA PODATKOV V PODJETJU 41

5.1 Strojna in programska infrastruktura 41
5.2 Organizacija podatkov na lokalnih sistemih 42
5.3 Varnost lokalne infrastrukture 44
5.4 Postopki varnostnega kopiranja 45
5.5 Prednosti in slabosti obstoječe rešitve 46

6. ANALIZA OBLAČNEGA SHRANJEVANJA PODATKOV V PODJETJU 48

6.1 Podatki, shranjeni v oblačnem okolju 48
6.2 Varnost oblačnega shranjevanja podatkov v podjetju 49
6.3 Upravljanje dostopa v oblačnih sistemih 49
6.4 Omejitve in tveganja oblačnega shranjevanja podatkov 50

7. PRIMERJAVA LOKALNEGA IN OBLAČNEGA SISTEMA V PODJETJU 52

7.1 Primerjava varnosti 52
7.2 Primerjava dostopnosti in hitrosti dela 53
7.3 Primerjava stroškov 55
7.4 Primerjava nadzora in upravljanja 56
7.5 Ključne prednosti in slabosti obeh pristopov 57

8. VARNOSTNA ANALIZA IN OCENA TVEGANJ 59

8.1 Tveganja pri lokalni infrastrukturi 59
8.2 Tveganja pri oblačnem shranjevanju podatkov 60
8.3 Identifikacija ranljivosti v obstoječem sistemu 61
8.4 Threat-modeling: najverjetnejši scenariji 62
8.5 Vpliv kibernetskih incidentov na delovne procese 63

9. PREDLOGI IZBOLJŠAV 64

9.1 Predlagane varnostne nadgradnje 64
9.2 Optimizacija obstoječega načina dela 64
9.3 Izboljšave varnostnih kopij in dostopnih pravic 65
9.4 Ocena izvedljivosti in priporočila 66

10. RAZPRAVA 67

10.1 Interpretacija rezultatov 67
10.2 Omejitve raziskave 67

10.3 MOŽNOSTI NADALJNJEGA RAZISKOVANJA 68

11. SKLEP 69

12. LITERATURE IN VIRI 71

KAZALO SLIK

SLIKA 2.2.2-1: PRIMER OMREŽNE ARHITEKTURE SISTEMA NAS. 16

SLIKA 2.2.2-2: SHEMATSKI PRIKAZ DISKOV V KONFIGURACIJI RAID. 17

SLIKA 4.4-1: INFRASTRUKTURA OMREŽJA PODJETJA. 39

SLIKA 5.2.-1: RAZPOREDITEV MAP IN ORGANIZACIJA V LOKALNEM OMREŽJU PODJETJA. 44

KAZALO TABEL

TABELA 2.2.2: PRIMERJAVA RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 17

TABELA 2.3.1: PRIMERJAVA MODELOV OBLAČNIH STORITEV (IAAS, PAAS, SAAS) 200

TABELA 2.4.2: PRIMERJAVA LOKALNEGA IN OBLAČNEGA SHRANJEVANJA 24

TABELA 7.2: PRIMERJAVA DOSTOPNOSTI IN HITROSTI DELA PRI LOKALNEM IN OBLAČNEM SHRANJEVANJU PODATKOV 55

TABELA 7.5.: PRIMERJAVA LOKALNEGA IN OBLAČNEGA PRISTOPA 58

1. UVOD

1.1 Opis področja in kontekst raziskave

Biotehnološko okolje temelji na natančnem eksperimentalnem delu, raziskavah in razvoju postopkov, pri katerih nastaja velika količina občutljivih podatkov. Ti podatki vključujejo raziskovalne dokumente, protokole, rezultate analiz in druge vsebine, ki imajo neposreden vpliv na nadaljnji razvoj tehnologij, pri čemer predstavljajo pomemben del intelektualne lastnine podjetja. Zaradi njihove poslovne in raziskovalne vrednosti je varno shranjevanje pomemben element delovanja podjetja.

V takšnem okolju je zanesljivo upravljanje podatkov pomembno za zagotavljanje sledljivosti, zaščite informacij ter neprekinjenega poteka raziskovalnega dela. Lokalni strežniki in oblačne storitve predstavljajo dva različna pristopa k shranjevanju podatkov, vsak s svojimi prednostmi in tveganji. Razumevanje teh razlik je bistvenega pomena za zagotavljanje ustrezne varnosti in podpore raziskovalnim procesom.

1.2 Problem varnega shranjevanja podatkov v biotehnološkem okolju

Biotehnološko okolje proizvaja občutljive raziskovalne, eksperimentalne in operativne podatke, ki imajo visoko poslovno vrednost in predstavljajo pomemben del intelektualne lastnine podjetja. Zaradi narave dela je tveganje razkritja, izgube ali nepooblaščenega dostopa do podatkov večje kot v številnih drugih panogah. Vsaka nenamerna sprememba ali izguba kritičnih dokumentov lahko vpliva na potek raziskav, razvoj tehnologij in konkurenčno prednost podjetja.

Podjetja v takšnem okolju morajo izbirati med lokalnim in oblačnim shranjevanjem podatkov, pri čemer vsak pristop vključuje specifična varnostna tveganja. Lokalni strežniki zagotavljajo večji nadzor nad občutljivimi podatki, vendar zahtevajo ustrezno upravljanje, zaščito in redno vzdrževanje. Oblačne storitve omogočajo lažje sodelovanje, a predstavljajo večjo izpostavljenost zunanjim grožnjam in nadzor zunanjega ponudnika nad podatki.

Zaradi kritične narave podatkov, omejenega dela od doma in neželenega zunanjega dostopa je ključni problem podjetja zagotoviti shranjevanje podatkov na način, ki hkrati podpira raziskovalni proces in zmanjšuje varnostna tveganja na najmanjšo možno raven.

1.3 Pomen podatkov v procesih celičnih terapij

Podatki imajo ključno vlogo v vseh fazah celičnih terapij, saj se na njihovi podlagi načrtujejo, izvajajo in ocenjujejo laboratorijski postopki. Pri delu s celicami nastajajo protokoli, rezultati eksperimentov, meritve, analize in spremljevalna dokumentacija, ki skupaj omogočajo sledljivost, ponovljivost in razvoj novih pristopov. Vsaka sprememba ali izguba podatkov lahko vpliva na potek raziskav in odločitve, ki temeljijo na preteklih rezultatih.

Zanesljivo shranjevanje podatkov zagotavlja neprekinjen potek raziskovalnih procesov in preprečuje tveganja, povezana z napakami, napačnimi interpretacijami ali zastoji pri delu. Ker so podatki pri celičnih terapijah pogosto občutljive narave in povezani z razvojem edinstvenih metod ter tehnologij, predstavljajo pomemben element intelektualne lastnine. Zato je njihova zaščita bistvena za ohranjanje konkurenčne prednosti in nadaljnji razvoj.

1.4 Namen, cilji in raziskovalna vprašanja

Namen diplomskega dela je predstaviti in analizirati varnostne vidike lokalnega in oblačnega shranjevanja podatkov v biotehnološkem okolju. Ker podjetje pri svojem delu ustvarja občutljive raziskovalne, eksperimentalne in operativne podatke, je izbira ustreznega načina shranjevanja ključna za ohranjanje zanesljivosti, zaščite informacij in neprekinjenega poteka raziskovalnega dela. Diplomsko delo obravnava prednosti in slabosti obeh pristopov ter ocenjuje, kateri način najprimerneje podpira varnostne potrebe podjetja.

Cilji diplomskega dela so:

- opisati vrste podatkov, ki se shranjujejo v podjetju, in način njihove razporeditve med lokalno in oblačno infrastrukturo,
- proučiti dejavnike, ki vplivajo na odločanje med lokalnim in oblačnim shranjevanjem,
- analizirati varnostne mehanizme posameznih pristopov in izpostaviti njihove prednosti ter omejitve,
- oceniti tveganja, povezana s shranjevanjem občutljivih podatkov,
- na podlagi ugotovitev pripraviti predloge izboljšav.

Raziskovalna vprašanja:

- Katere vrste podatkov se shranjujejo na lokalnih strežnikih in katere v oblačnih storitvah?
- Katere dejavnike podjetje upošteva pri odločitvi za lokalno ali oblačno shranjevanje?
- Kako so urejeni varnostni postopki za zaščito podatkov v podjetju?
- Katera so glavna tveganja pri uporabi lokalnih in oblačnih rešitev?
- Kako podjetje zagotavlja zaščito podatkov pred izgubo, nepooblaščenim dostopom ali spremembami?
- Kako bi bilo mogoče obstoječi sistem shranjevanja podatkov izboljšati z vidika varnosti in učinkovitosti?

1.5 Metodologija raziskovalnega dela

Raziskava uporablja kombiniran pristop, ki združuje kvalitativne in kvantitativne metode. Kvalitativni del obsega pregled dokumentacije, strežniških nastavitev in postopkov shranjevanja podatkov, skupaj z neformalnimi razgovori z zaposlenimi. Kvantitativni del vključuje pregled obsega in razporeditve podatkov ter tehničnih značilnosti lokalnih in oblačnih sistemov. Jedro raziskave predstavlja primerjalna analiza, ki temelji na študiji primera dejanskega okolja podjetja.

1.6 Struktura diplomskega dela

Diplomsko delo je razdeljeno na več poglavij. V uvodnem delu so predstavljeni kontekst raziskave, problem varnega shranjevanja podatkov, pomen podatkov v procesih celičnih terapij ter namen, cilji in uporabljene raziskovalne metode. Drugo poglavje zajema teoretična izhodišča, povezana s podatkovnimi sistemi, lokalno infrastrukturo, oblačnimi storitvami, primerjavo obeh pristopov in kibernetsko varnostjo. Tretje poglavje predstavlja pregled regulativnih okvirov. V četrtem poglavju je opisan kontekst dela podjetja. Peto in šesto poglavje obravnavata analizo lokalnega in oblačnega shranjevanja podatkov v podjetju. Sedmo poglavje vsebuje primerjavo obeh pristopov, osmo pa varnostno analizo in oceno tveganj. Deveto poglavje vključuje predloge izboljšav. Sledita razprava in sklep, končni del pa sestavljajo literatura ter priloge.

2. TEORETIČNA IZHODIŠČA

2.1 Podatkovni sistemi v biotehnologiji

2.1.1 Vrste podatkov v laboratorijskem okolju

V biotehnološkem laboratoriju nastajajo različne vrste podatkov, ki spremljajo raziskovalno in razvojno delo. Sem spadajo eksperimentalni zapisi, protokoli, meritve, fotografska dokumentacija in analitični rezultati, ki odražajo potek in izid posameznih postopkov. Poleg raziskovalnih podatkov se shranjuje tudi administrativna dokumentacija, kot so delovne instrukcije, poročila, razvojni zapisi in tehnični dokumenti (Michael E. Whitman, 2014).

Operativni podatki zajemajo informacije o načrtovanju dela, organizaciji nalog in komunikaciji med zaposlenimi. Posebno skupino predstavljajo pravni in poslovni dokumenti, med katere sodijo pogodbe, interne smernice ter dokumentacija, povezana z intelektualno lastnino, ki se v informacijskih sistemih obravnavajo kot informacijska sredstva z različno stopnjo pomembnosti za delovanje organizacije (Peltier, 2001).

Različne skupine podatkov imajo različno vlogo v raziskovalnem procesu, zato morajo biti shranjene na način, ki omogoča jasen pregled, nadzor in enostavno uporabo pri nadaljnjem delu, kar predstavlja eno temeljnih načel upravljanja informacijskih sredstev v organizacijah (Imperva, 2025).

2.1.2 Občutljivost in kritičnost bioloških podatkov

Biološki podatki, ki nastajajo v laboratorijskem okolju, imajo pomembno raziskovalno in poslovno vrednost, saj predstavljajo temelj za razvoj, validacijo in izboljševanje raziskovalnih procesov (Michael E. Whitman, 2014). Gre za informacije, ki opisujejo rezultate eksperimentov, lastnosti bioloških vzorcev, potek laboratorijskih postopkov ter razvoj novih metod, zato imajo ključno vlogo pri nadaljnjem znanstvenem in tehnološkem delu. Zaradi svoje vsebine so takšni podatki pogosto neposredno povezani z intelektualno lastnino podjetja, saj odražajo znanje, postopke in rešitve, ki predstavljajo konkurenčno prednost organizacije (Peltier, 2001).

Občutljivost bioloških podatkov izhaja tudi iz njihovega neposrednega vpliva na raziskovalne postopke in interpretacijo rezultatov. Nepravilno shranjeni, izgubljeni ali nenamerno spremenjeni podatki lahko vodijo do napačnih zaključkov, ponavljanja poskusov ali nepravilnih odločitev v nadaljnjih fazah razvoja. Takšne napake lahko upočasnijo raziskovalni proces, povečajo stroške in negativno vplivajo na kakovost rezultatov. Poleg tega lahko razkritje občutljivih informacij pomeni izgubo konkurenčne prednosti, saj omogoča dostop do razvojnih idej, postopkov ali tehničnih rešitev nepooblaščenim osebam (Michael E. Whitman, 2014).

Stopnja kritičnosti bioloških podatkov je zato tesno povezana z njihovim vplivom na raziskave, razvoj tehnologije in poslovno delovanje podjetja. Zaradi tega morajo biti takšni podatki ustrezno zaščiteni pred nepooblaščenim dostopom, nenamernimi spremembami ali izgubo. Hkrati morajo biti organizirani na način, ki omogoča preglednost, sledljivost in zanesljivo uporabo v celotnem raziskovalnem procesu, kar predstavlja eno temeljnih načel upravljanja informacijskih sredstev v organizacijah (Imperva, 2025).

2.1.3 Zahteve za sledljivost in arhiviranje podatkov

Sledljivost podatkov predstavlja pomemben element laboratorijskega dela, saj omogoča pregled nad izvajanjem posameznih postopkov, ponovno analizo rezultatov ter razumevanje razvoja in sprememb v poteku eksperimentov. Zanesljiva sledljivost zagotavlja, da je mogoče za vsak podatek ugotoviti njegov izvor, čas nastanka in povezavo z določenim postopkom ali eksperimentalno fazo, kar je ključno za ponovljivost raziskav in presojo njihove kakovosti (Council of Europe, 2012). Da je sledljivost zagotovljena, morajo biti podatki shranjeni na način, ki omogoča pregledno označevanje, enostavno iskanje ter dostop do preteklih zapisov. Pomembno je tudi, da so podatki organizirani po logični strukturi, ki odraža potek dela in posamezne faze raziskovalnega procesa (Michael E. Whitman, 2014)

Arhiviranje podatkov je tesno povezano z zagotavljanjem dolgoročne dostopnosti informacij, ki se lahko uporabijo pri kasnejših analizah, preverjanju rezultatov ali ponovitvah postopkov. Namen arhiviranja ni zgolj shranjevanje podatkov, temveč tudi ohranjanje njihove celovitosti, točnosti in nespremenjenosti skozi čas. Podatki morajo biti zato shranjeni v stabilnem in zanesljivem okolju, ki omogoča zaščito pred izgubo, poškodbami ali nepooblaščenimi spremembami (Council of Europe, 2012). Arhivni podatki morajo biti jasno ločeni od podatkov,

ki se še aktivno obdelujejo, saj se s tem zmanjša tveganje nenamernega spreminjanja ali brisanja informacij.

Z ustrezno urejeno sledljivostjo in arhiviranjem podatkov je omogočeno strukturirano delo, večja preglednost nad informacijami ter učinkovitejši nadzor nad raziskovalnimi procesi. Takšen pristop omogoča ohranjanje podatkov, ki lahko vplivajo na nadaljnji razvoj raziskav, ter podpira odgovorno upravljanje informacijskih sredstev v laboratorijskem in raziskovalnem okolju (Wikepedia, n.d).

2.2 Lokalna IT-infrastruktura

2.2.1 Lokalni strežniki – arhitektura in delovanje

Lokalni strežniki predstavljajo osrednji del informacijske infrastrukture podjetja, saj omogočajo shranjevanje, obdelavo in upravljanje podatkov znotraj internega omrežja organizacije. Takšen pristop omogoča centraliziran nadzor nad podatki ter zmanjšuje odvisnost od zunanjih ponudnikov storitev, kar je še posebej pomembno v okoljih z višjimi zahtevami glede varnosti in razpoložljivosti informacij (Brelih, 2019). Lokalna infrastruktura se pogosto uporablja v organizacijah, kjer je potreben neposreden nadzor nad podatki ter predvidljivo delovanje informacijskih sistemov (Jungco, 2025).

Arhitektura lokalnih strežnikov temelji na kombinaciji strojne in programske opreme, ki skupaj omogočata izvajanje datotečnih storitev, upravljanje uporabnikov in podporo aplikacijam za vsakodnevne delovne procese. Strojna zasnova običajno vključuje procesor, pomnilnik, omrežne vmesnike in diskovne enote, ki so lahko povezane v različne konfiguracije za zagotavljanje večje zanesljivosti in razpoložljivosti sistema. Strežniki so preko kabelskih ali optičnih povezav vključeni v interno omrežje, ki ga sestavljajo stikala, usmerjevalniki in druga omrežna oprema, kar omogoča dostop do podatkov znotraj organizacije brez posredovanja zunanjih omrežij (Jelenc, 2023).

Programsko okolje lokalnega strežnika vključuje operacijski sistem ter podporne storitve, kot so datotečni strežniki, sistemi za upravljanje uporabniških pravic, nadzor dostopa in diagnostična orodja. Skrbniki sistema imajo možnost upravljanja strukture map, dodeljevanja dostopnih pravic ter spremljanja delovanja in obremenitve strežniškega sistema. Takšen način

delovanja omogoča učinkovito upravljanje informacij ter hkratno uporabo podatkov s strani več uporabnikov, ob ohranjanju nadzora nad spremembami in dostopi (National Institute of Standards and Technology, 2018).

Ena izmed značilnosti lokalnih strežnikov je, da vsi podatki ostajajo znotraj internega omrežja podjetja, kar zmanjšuje tveganja, povezana s prenosom podatkov prek zunanjih omrežij. Hitrost dostopa do podatkov ni neposredno odvisna od internetne povezave ali razpoložljivosti zunanjih storitev, kar prispeva k stabilnosti delovanja sistema. Lokalna infrastruktura omogoča tudi integracijo z dodatnimi varnostnimi mehanizmi, kot so sistemi za varnostne kopije, avtentikacijo in spremljanje delovanja, kar podpira zahteve po varnosti in nadzoru nad podatki (Carbide, n.d).

2.2.2 Sistemi NAS, RAID in redundanca

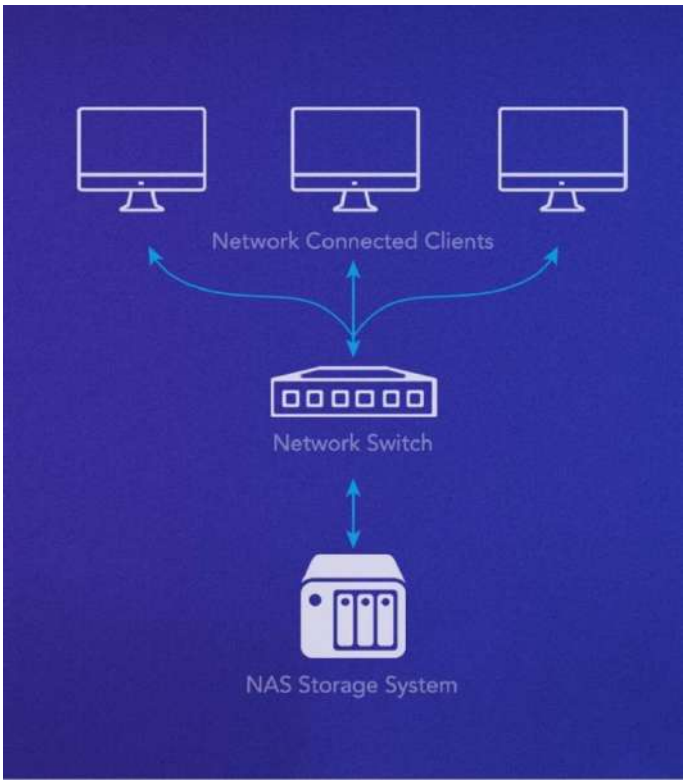
Sistemi NAS (Network Attached Storage) so samostojne shranjevalne enote, ki se v omrežje povezujejo kot ločene naprave in omogočajo centralizirano shranjevanje podatkov. Namenjeni so zagotavljanju dostopa do datotek prek omrežnih protokolov, kot sta SMB ali NFS, ter omogočajo večuporabniško delo v skupnih mapah. NAS sistemi imajo lasten operacijski sistem, ki omogoča upravljanje map, uporabnikov in dostopnih pravic, zaradi česar lahko delujejo neodvisno od klasičnih strežniških rešitev (Backblaze, 2023).

Ker NAS naprave praviloma uporabljajo več diskov, se pogosto povezujejo s konfiguracijami RAID (Redundant Array of Independent Disks), ki izboljšujejo zanesljivost shranjevanja podatkov. Tehnologija RAID omogoča združevanje več diskov v eno logično enoto, pri čemer se podatki razporedijo tako, da se zmanjša tveganje izgube podatkov ob okvari posameznega diska. Različni nivoji RAID uporabljajo različne pristope razporejanja podatkov in paritetnih informacij. RAID 1 na primer zagotavlja zrcaljenje podatkov, medtem ko RAID 5 združuje podatke in pariteto ter omogoča obnovo podatkov ob okvari enega diska (Pandora FMS team |, 2021).

Koncept redundance opisuje uporabo več komponent, kot bi jih bilo nujno potrebnih za osnovno delovanje sistema. Pri shranjevanju podatkov to pomeni, da so informacije razporejene tako, da ob okvari posameznega diska ali dela sistema ne pride do izgube podatkov. Redundanca prispeva k večji dostopnosti podatkov, zmanjševanju tveganja izgube informacij ter stabilnemu

delovanju shranjevalnega okolja, kar je pomembno zlasti v lokalnih informacijskih sistemih (National Institute of Standards and Technology, 2018).

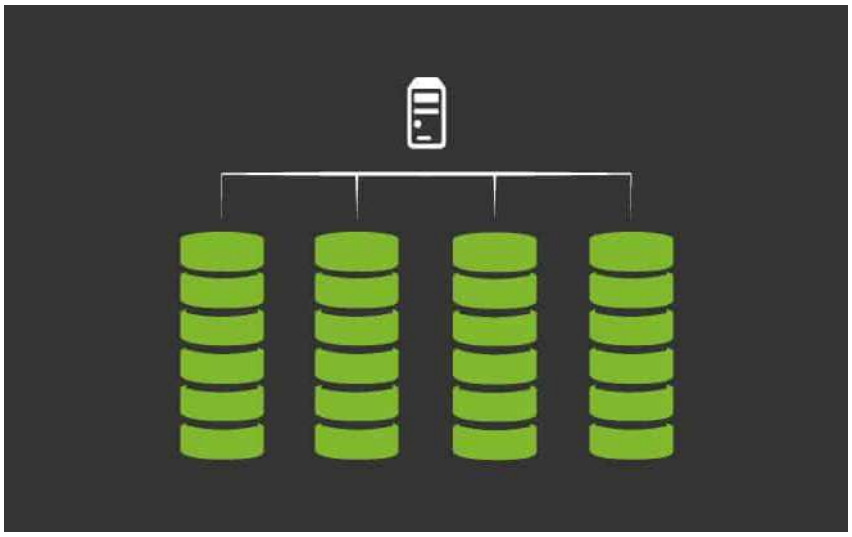
Na spodnji sliki je prikazan poenostavljen primer arhitekture sistema NAS. Uporabniki so povezani v notranje omrežje preko stikala, shranjevalna enota pa deluje kot osrednja točka za dostop do podatkov.



Slika 2.2.2-1: Primer omrežne arhitekture sistema NAS.

Vir: (Backblaze, 2023)

Ker sistemi NAS običajno uporabljajo več diskov, se za večjo zanesljivost uporablja ena izmed konfiguracij RAID. Spodnja slika prikazuje osnovno strukturo razporeditve diskov v polju RAID (J. Donelly, 2023).



Slika 2.2.2-2: Shematski prikaz diskov v konfiguraciji RAID.

Vir: (Pandora FMS team |, 2021)

Tabela 2.2.2: Primerjava RAID 0, RAID 1, RAID 5, RAID 6, RAID 10

RAID nivo	**Način delovanja**	**Prednost**	**Slabost**
RAID 0	Razdelitev podatkov brez redundance	visoka hitrost	ob okvari izguba podatkov
RAID 1	Zrcaljenje podatkov	podatki ostanejo dostopni ob okvari	polovična kapaciteta
RAID 5	Podatki + pariteta	dobra kombinacija zaščite in prostora	obnova po okvari je počasnejša
RAID 6	Dvojna pariteta	zaščita ob okvari dveh diskov	nižje hitrosti pisanja
RAID 10	RAID 1 + 0	hitrost + redundanca	visoka poraba prostora

Vir: Lastna priprava

Sistemi NAS v kombinaciji z ustrezno konfiguracijo RAID zagotavljajo stabilno in razširljivo okolje za shranjevanje podatkov v lokalnih infrastrukturnih sistemih (J. Donelly, 2023).

2.2.3 Prednosti in slabosti lokalne infrastrukture

Lokalna infrastruktura temelji na strežnikih in shranjevalnih enotah, ki delujejo znotraj internega omrežja organizacije. Ena izmed prednosti takšnega pristopa je neposreden nadzor nad podatki, saj celotno okolje deluje neodvisno od zunanjih ponudnikov (Cloudfresh, 2024). Podatki ostanejo v fizičnem prostoru organizacije, kar omogoča strožjo kontrolo nad dostopom in razporeditvijo pravic (Cloudfresh, 2024). Hitrost dostopa do podatkov ni odvisna od internetne povezave, temveč od zmogljivosti lokalnega omrežja, kar omogoča stabilno delovanje pri vsakodnevni uporabi.

Lokalno okolje omogoča tudi prilagoditev shranjevalnih in strežniških sistemov glede na potrebe dela. Organizacija lahko določa strukturo map, način razporeditve podatkov in uporabniške vloge, kar prispeva k preglednosti in enostavnejši organizaciji delovnih procesov (Garbe, 2025). V primeru nadgradenj ali sprememb v poteku dela je možno opremo in konfiguracije prilagoditi brez zunanjih omejitev (Garbe, 2025).

Slabost lokalne infrastrukture je potreba po rednem vzdrževanju ter spremljanju delovanja strojne in programske opreme (Ial, 2024). Zahtevano je sprotno posodabljanje, preverjanje delovanja diskov, upravljanje varnostnih kopij in skrb za omrežno opremo. V primeru okvare strežniških komponent lahko pride do začasne nedostopnosti podatkov, čeprav se to tveganje bistveno zmanjša z redundanco in ustreznimi postopki varnostnega kopiranja. Z rastjo količine podatkov je potrebna tudi postopna nadgradnja strojnih kapacitet, kar predstavlja dodatni strošek in zahteva načrtovanje (Ial, 2024).

2.2.4 Varnostni mehanizmi lokalnih sistemov

Lokalni sistemi uporabljajo več varnostnih mehanizmov, ki skupaj omogočajo nadzor nad dostopom in zaščito podatkov (Boško, 2025). Prvi element predstavljajo uporabniške pravice, ki določajo, kdo lahko dostopa do posameznih map ali datotek. Uporabniki so razdeljeni v

skupine, njihov dostop pa se upravlja preko nastavitev na strežniku, kar omogoča omejitev dostopa le na pooblaščene uporabnike (Boško, 2025). Takšen nadzor omogoča pregledno razmejitev med različnimi vlogami v organizaciji.

Poleg upravljanja pravic se lokalni sistemi zanašajo na ločitev omrežij in nadzor nad notranjim prometom (network segmentation), kar povečuje varnost omrežja z omejevanjem širjenja napadov in znižuje možnost nepooblaščenega dostopa do občutljivih podatkov (Chin, 2026); (Enterprise Networking Planet, 2023). Strežniki delujejo v zaščitenem delu omrežja, do katerega je dostop mogoč samo iz naprav, ki so vključene v interno omrežje, s tem pa so podatki ločeni od zunanjega omrežja.

Pomemben varnostni element je tudi nadzor nad delovanjem strežnikov. To vključuje spremljanje obremenitev, delovanja diskov, razpoložljivega prostora in posodobitev programske opreme, saj redno spremljanje pomaga hitro zaznati potencialne napake ali varnostne incidente ter omogoča pravočasno odzivanje (Trio, 2025).

Varnost lokalnih sistemov dopolnjujejo še varnostne kopije, ki omogočajo obnovo podatkov v primeru okvare ali nenamernega brisanja. Kopije se lahko shranjujejo na ločene naprave ali na namenski sistem za varnostne kopije, kar zmanjšuje tveganje sočasne izgube podatkov zaradi strojne okvare ali nesreče (INTROSERV, n.d.).

2.3 Oblačne storitve

2.3.1 Osnovni modeli oblačnih storitev (IaaS, PaaS, SaaS)

Oblačne storitve so razdeljene na več modelov, ki se razlikujejo glede na stopnjo nadzora, ki ga uporabnik ohrani nad infrastrukturo in aplikacijami (IBM, n.d.). Najpogosteje uporabljeni so modeli IaaS, PaaS in SaaS, ki se uporabljajo v različnih informacijskih okoljih (IBM, n.d.).

Model IaaS (Infrastructure as a Service) omogoča uporabo osnovne infrastrukture v oblaku, kot so strežniki, diskovni prostor in mrežne komponente (IBM, n.d.). Uporabnik upravlja programsko opremo, podatke in aplikacije, medtem ko ponudnik skrbi za fizično infrastrukturo, virtualizacijo in omrežje (Google Cloud, n.d.). Ta pristop omogoča fleksibilnost pri konfiguraciji in skaliranju zmogljivosti.

Model PaaS (Platform as a Service) vključuje infrastrukturo in dodatno programsko okolje, ki je namenjeno razvoju in izvajanju aplikacij (IBM, n.d.). Uporabniku ni treba upravljati strežnikov ali sistemskih nastavitev, saj platforma nudi pripravljeno okolje za delo, kar zmanjšuje kompleksnost upravljanja osnovnih sistemskih komponent (Google Cloud, n.d.). Primeren je za razvojne procese, kjer je potrebna enotna in nadzorovana platforma.

Model SaaS (Software as a Service) predstavlja popolnoma upravljano storitev, kjer uporabnik dostopa do aplikacije, ki jo v celoti upravlja ponudnik (IBM, n.d.). Podatki, strežniški sistemi in delovanje aplikacije se nahajajo v oblaku, uporabnik pa uporablja aplikacijo preko spletnega vmesnika ali namenske programske opreme (Google Cloud, n.d.). Ta model je razširjen pri orodjih za komunikacijo, produktivnost in organizacijo dela, saj omogoča uporabo funkcionalnih aplikacij brez potrebe po upravljanju infrastrukture ali platforme.

Tabela 2.3.1: Primerjava modelov oblačnih storitev (IaaS, PaaS, SaaS)

Model	Kaj nudi	Kaj upravlja uporabnik
IaaS	infrastruktura	OS, aplikacije, podatki
PaaS	infrastruktura + platforma	aplikacije in podatki
SaaS	celotna aplikacija	samo uporabo aplikacije

Vir: Lastna priprava

2.3.2 Prednosti in slabosti oblačnih rešitev

Oblačne storitve omogočajo dostop do aplikacij in podatkov po internetu, kar zagotavlja prilagodljivost in enostavno vključevanje v različna delovna okolja. Ena izmed prednosti takšnega pristopa je možnost dostopa ne glede na lokacijo uporabnika, kar olajša sodelovanje in izmenjavo informacij. Ponudnik storitve skrbi za infrastrukturo, posodobitve in vzdrževanje, kar zmanjša potrebo po lastnih strojnih in programskih virih (Perhavec, 2022).

Med prednosti oblačnih rešitev sodijo tudi prilagodljiva poraba virov, enostavno skaliranje in uporaba storitev po načelu sprotnega plačevanja. Ob tem je omogočeno hitro uvajanje novih aplikacij in nadgraditev, brez posegov v lokalno infrastrukturo (Perhavec, 2022).

Slabost oblačnih rešitev je odvisnost od internetne povezave, saj dostop do podatkov ni mogoč v primeru izpada ali omejene povezljivosti. Dodatno je za varnost podatkov odgovoren zunanji ponudnik, kar zmanjšuje neposreden nadzor nad shranjenimi informacijami. Pri uporabi oblačnih storitev je treba upoštevati tudi možnost geografskega shranjevanja podatkov in politike ponudnika glede zasebnosti ter obdelave informacij (Perhavec, 2022).

2.3.3 Varnostni mehanizmi v oblaku

Ponudniki oblačnih storitev uporabljajo različne varnostne mehanizme, ki omogočajo zaščito podatkov in zagotavljajo stabilno delovanje njihovih storitev. Eden izmed osnovnih mehanizmov je avtentikacija uporabnikov, ki vključuje preverjanje identitete preko gesel, večfaktorskega preverjanja ali integracije z drugimi sistemi za upravljanje identitet. Na ta način je dostop do podatkov in aplikacij omejen na uporabnike z ustreznimi dovoljenji (Perhavec, 2022).

Pri shranjevanju podatkov se pogosto uporablja šifriranje, tako pri prenosu kot v mirovanju. Šifriranje pri prenosu podatkov preprečuje prestrezanje vsebine med komunikacijo, medtem ko šifriranje v mirovanju zmanjšuje tveganje nepooblaščenega dostopa do podatkov, ki so shranjeni na strežnikih ponudnika. Ti pristopi omogočajo dodatno plast zaščite ne glede na lokacijo shranjevanja (Perhavec, 2022).

Varnostni mehanizmi vključujejo tudi nadzor nad dostopom in evidentiranje aktivnosti. Ponudniki oblačnih storitev omogočajo beleženje sprememb, prijav in drugih dejanj, kar omogoča pregled nad delovanjem sistema in hitrejše odkrivanje nepravilnosti. Poleg tega se uporabljajo sistemi za zaznavanje napak, spremljanje delovanja in vzdrževanje infrastrukture, ki skrbijo za razpoložljivost in stabilnost storitev (Perhavec, 2022).

Pri oblačnih okoljih so pogosto vključeni tudi postopki za obnavljanje podatkov, ki omogočajo povrnitev vsebine v primeru tehničnih težav ali nenamernih sprememb. Ti postopki so usklajeni s politikami, ki jih določa ponudnik in jih je mogoče prilagoditi potrebam posameznih uporabnikov (Perhavec, 2022).

2.3.4 Tipična uporaba oblaka v podjetjih

Podjetja uporabljajo oblačne storitve predvsem zaradi enostavnega dostopa do aplikacij in podatkov ter manjše potrebe po lastni infrastrukturi. Običajna uporaba vključuje orodja za komunikacijo, načrtovanje dela, upravljanje dokumentov in izmenjavo datotek, saj so te storitve dostopne z različnih lokacij. Oblačne platforme omogočajo sodelovanje več uporabnikov hkrati in s tem olajšajo delo v okoljih, kjer se naloge izvajajo v skupinah (Perhavec, 2022).

Poleg komunikacijskih orodij se oblak uporablja za shranjevanje dokumentov, arhiviranje podatkov in upravljanje nalog. Takšen pristop je pogost v organizacijah, ki želijo zmanjšati obremenitev lastne infrastrukture ali omogočiti enostavno razširitev prostora glede na potrebe dela. V nekaterih primerih se oblak uporablja za razvojna ali testna okolja, saj omogoča hitro vzpostavitev sistemov brez dodatne strojne opreme (Perhavec, 2022).

V raziskovalnih in biotehnoloških okoljih se oblak najpogosteje uporablja za komunikacijo, izmenjavo dokumentacije in organizacijo dela, medtem ko se podatki, ki zahtevajo višjo stopnjo nadzora, običajno hranijo v lokalnih sistemih (Neng W., 2025).

2.4 Primerjava lokalnega in oblačnega shranjevanja

Lokalno in oblačno shranjevanje podatkov predstavljata dva različna pristopa, ki se razlikujeta po nadzoru nad podatki, arhitekturi, stroških ter načinu dostopa. Izbira med njima je odvisna od potreb organizacije, stopnje občutljivosti podatkov in razpoložljivih virov za upravljanje informacijskih sistemov. Ker se v raziskovalnih in biotehnoloških okoljih pojavljajo podatki z visoko vrednostjo in potrebe po nadzorovanem dostopu, je primerjava obeh pristopov pomembna za razumevanje njihovih prednosti in omejitev (Perhavec, 2022).

2.4.1 Razlike v nadzoru in arhitekturi

Pri lokalnem shranjevanju podatkov organizacija sama upravlja strežnike, shranjevalne enote in celotno podatkovno okolje. Podatki se nahajajo znotraj internega omrežja, kar omogoča neposreden nadzor nad tem, kje so shranjeni in kdo lahko do njih dostopa. Arhitektura je postavljena na internih strežnikih, ki jih upravljajo zaposleni z ustreznimi pravicami. To vključuje dodeljevanje dostopov, organizacijo map, spremljanje delovanja ter načrtovanje

nadgradenj. Lokalna arhitektura tako zagotavlja jasno razmejitev vlog in preglednost nad podatkovnimi tokovi (P. Diamond, 2020).

Pri oblačnem shranjevanju je fizična infrastruktura zunaj organizacije, v podatkovnih centrih ponudnikov storitev. Arhitekturo vzpostavi in upravlja ponudnik, uporabniki pa dostopajo do podatkov preko spleta. Nastavitve delovanja, razporejanje zmogljivosti in vzdrževanje niso v domeni organizacije, ampak so del storitve, ki jo nudi ponudnik. To pomeni, da ima uporabnik dostop do podatkov, ne pa tudi do nadzora nad fizičnim okoljem, v katerem se ti podatki nahajajo (P. Diamond, 2020).

Razlika med obema pristopoma se kaže predvsem v nadzoru nad podatkovnim življenjskim ciklom. Lokalni sistem omogoča neposredno upravljanje arhitekture in popoln vpogled v njen potek, kar je uporabno v okoljih, kjer se obdelujejo podatki, ki zahtevajo večjo preglednost. Pri oblačnih rešitvah pa je nadzor nad arhitekturo omejen na funkcionalnosti, ki jih omogoča ponudnik, kar lahko vpliva na odločitev organizacij, ki potrebujejo višjo stopnjo notranjega upravljanja (P. Diamond, 2020).

2.4.2 Razlike v stroških, dostopu in uporabi

Stroški lokalnega shranjevanja podatkov so povezani predvsem z nakupom strojne opreme, vzdrževanjem in nadgradnjami informacijskega sistema. Organizacija mora zagotoviti strežnike, shranjevalne enote ter omrežno opremo, kar predstavlja višji začetni finančni vložek. Poleg tega je potrebno redno spremljanje delovanja, posodabljanje sistemov in upravljanje varnostnih kopij. Takšni stroški so praviloma bolj predvidljivi, vendar se pojavljajo v večjih časovnih intervalih, zlasti ob nadgradnjah ali razširitvah sistema (Neng W., 2025).

Pri oblačnem shranjevanju podatkov so stroški razdeljeni glede na sprotno uporabo storitev, kar vključuje plačilo za zakupljeni prostor, dodatne storitve ali število uporabnikov. Organizacija ne potrebuje lastne infrastrukture in ne skrbi za fizično opremo, kar lahko zmanjša stroške vzdrževanja. Kljub temu je pri dolgoročni uporabi treba upoštevati, da se lahko ob povečevanju obsega storitev ali števila uporabnikov skupni stroški postopoma zvišujejo (Neng W., 2025).

Razlike med lokalnim in oblačnim shranjevanjem se kažejo tudi v dostopu do podatkov. Lokalni sistemi omogočajo dostop predvsem znotraj internega omrežja, kar zagotavlja stabilno delovanje neodvisno od zunanje internetne povezave. Oblačno shranjevanje pa omogoča dostop

do podatkov z različnih lokacij in naprav, vendar je ta dostop neposredno odvisen od internetne povezave ter razpoložljivosti storitev ponudnika (Jungco, 2025).

Pri uporabi sta obravnavana pristopa prav tako različna. Lokalni sistemi se pogosteje uporabljajo za shranjevanje podatkov, ki zahtevajo višjo stopnjo nadzora, preglednosti in omejen dostop. Oblačne storitve pa se pogosteje uporabljajo za komunikacijo, organizacijo dela in izmenjavo dokumentov, kjer sta ključni dostopnost in sodelovanje med uporabniki (Neng W., 2025).

Tabela 2.4.2: Primerjava lokalnega in oblačnega shranjevanja

Vidik	**Lokalno shranjevanje**	**Oblačno shranjevanje**
Stroški	višji začetni stroški, vzdrževanje znotraj organizacije	sprotno plačevanje, brez lastne strojne opreme
Dostop	dostop omejen na interno omrežje	dostop preko interneta
Uporaba	primerno za občutljive podatke in nadzorovano okolje	primerno za komunikacijo, sodelovanje in delo na daljavo

Vir: Lastna priprava

2.4.3 Analiza tveganj

Pri primerjavi lokalnega in oblačnega shranjevanja podatkov je pomembno razumeti tveganja, ki so povezana z vsakim pristopom. Tveganja se razlikujejo glede na način upravljanja infrastrukture, dostopnost podatkov ter stopnjo nadzora nad informacijami.

Pri lokalnem shranjevanju se tveganja nanašajo predvsem na delovanje strojne opreme, upravljanje varnostnih kopij in vzdrževanje sistema. Okvara diskov, omrežne opreme ali strežnika lahko začasno omeji dostop do podatkov, zato so pomembni postopki varnostnega kopiranja in redundanca. Poleg tega je treba zagotoviti redno posodabljanje programske opreme in nadzor nad delovanjem, saj teh nalog ne prevzema noben zunanji ponudnik. Nepravilno upravljanje ali pomanjkljiva organizacija dostopnih pravic lahko vpliva na zanesljivost delovanja in varnost podatkov (Michael E. Whitman, 2014).

Pri oblačnem shranjevanju se tveganja nanašajo predvsem na zunanjo infrastrukturo. Ker podatki niso v fizičnem prostoru organizacije, je dostop do njih odvisen od internetne povezljivosti ter delovanja ponudnikove storitve. Možne so prekinitve zaradi vzdrževalnih posegov, izpadov storitve ali tehničnih težav na strani ponudnika. Dodatno tveganje predstavlja deljeni nadzor nad podatki, saj se del varnostnih postopkov izvaja na infrastrukturi, ki ni neposredno pod upravljanjem organizacije (Perhavec, 2022).

V okoljih, kjer se uporabljajo podatki z višjo stopnjo občutljivosti, je treba upoštevati tudi morebitna tveganja pri nepooblaščenem dostopu ali nejasno določenih politikah ravnanja s podatki. Pri oblačnih storitvah je pomembno pregledati, kako ponudnik obravnava shranjevanje, šifriranje in obdelavo podatkov, ter kakšne so možnosti za povrnitev podatkov v primeru izgube ali napake v storitvi (Neng W., 2025).

Čeprav se tveganja razlikujejo, jih je v obeh pristopih mogoče obvladovati z ustrezno organizacijo, nadzorom in varnostnimi postopki. Pri tem je pomembno izbrati način shranjevanja, ki najbolj ustreza potrebam dela, zahtevam po nadzoru in zanesljivosti ter stopnji občutljivosti podatkov.

2.5 Kibernetska varnost

Kibernetska varnost obravnava postopke in pristope za zaščito informacijskih sistemov pred motnjami, zlorabami ali nepooblaščenim dostopom. Ker sodobni informacijski sistemi temeljijo na stalni povezanosti z omrežji in storitvami, je upravljanje varnosti del rednega delovanja vsake organizacije. Varnostni ukrepi se nanašajo na zaščito podatkov, nemoteno delovanje sistemov in nadzor nad tem, kako uporabniki dostopajo do informacij (Microsoft, 2026).

Informacijski sistemi vključujejo strežnike, shranjevalne enote in komunikacijske poti, zato lahko do težav pride zaradi tehničnih napak, napak pri ravnanju uporabnikov ali namernih poskusov zlorab. Namen kibernetske varnosti je sistematično prepoznavanje takšnih tveganj ter vzpostavitev postopkov, ki zmanjšujejo možnost napak in omejijo vpliv nepravilnosti na delovanje organizacije. V okoljih, kjer se hranijo ali obdelujejo podatki z večjo občutljivostjo, je pomembno, da so postopki nadzora jasno določeni in dosledno izvedeni (Investopedia , 2017).

Za vzdrževanje varnega delovanja informacijskih sistemov se uporabljajo tehnični in organizacijski ukrepi. Med tehničnimi ukrepi so upravljanje uporabniških pravic, nadzor dostopa, posodobitve programske opreme, šifriranje in spremljanje delovanja omrežij. Organizacijski ukrepi vključujejo določene postopke za ravnanje z dostopi, prijavo incidentov ter redno preverjanje, ali se varnostni postopki izvajajo v praksi. Kombinacija teh pristopov omogoča preglednost nad delovanjem sistemov in zmanjša verjetnost, da bi prišlo do izgube podatkov ali prekinitve delovanja (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

V nadaljevanju so predstavljeni najpogostejši tipi groženj ter ukrepi, ki jih organizacije uporabljajo za njihovo zmanjševanje, skupaj z mehanizmi, ki podpirajo zanesljivo in pregledno obdelavo podatkov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

2.5.1 Vrste groženj

Grožnje v informacijskih sistemih se pojavljajo zaradi tehničnih napak, neustreznega ravnanja uporabnikov ali namernih poskusov zlorab. Namen razvrščanja groženj je razumevanje, od kod lahko izvirajo težave in kako lahko vplivajo na delovanje sistema. Grožnje lahko obravnavamo v več skupinah, pri čemer se posamezne kategorije med seboj prekrivajo, vendar omogočajo pregled nad najpogostejšimi vzroki za motnje v delovanju informacijskih okolij (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Ena skupina groženj so tehnične okvare in napake v delovanju opreme. Sem sodijo okvare diskov, napake na strežnikih, izpadi električne energije, nepravilno delovanje omrežne opreme ali programske napake, ki vplivajo na dostopnost podatkov. Takšne grožnje lahko povzročijo izgubo podatkov ali nepričakovane prekinitve delovanja, zato so pomembni postopki vzdrževanja, spremljanja in varnostnega kopiranja (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Pomembna skupina groženj je povezana s človeškim faktorjem. Uporabniki lahko nenamerno izbrišejo podatke, napačno nastavijo pravice dostopa ali ravnajo v nasprotju s postopki. Poleg nenamernih napak se pojavljajo tudi primeri nepooblaščenega dostopa ali poskusov pridobivanja informacij, kjer posamezniki izkoristijo pomanjkljivosti v organizaciji dela ali pomanjkanje nadzora. Človeški faktor je prisoten v vseh informacijskih okoljih, zato je pomembno, da so postopki opredeljeni jasno in da uporabniki razumejo, kako ravnati z dostopnimi podatki (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

H grožnjam sodijo tudi zlonamerne dejavnosti, kot so poskusi vdorov v sisteme, širjenje škodljive programske opreme ali poskusi pridobivanja gesel z uporabo različnih tehnik. Takšne grožnje lahko povzročijo nepooblaščen dostop do podatkov, okvare sistemov ali širše motnje v delovanju omrežja. Obramba pred takimi napadi zahteva kombinacijo tehničnih ukrepov, nadzora in pravilnega ravnanja uporabnikov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Nekatera tveganja izvirajo tudi iz organizacijskih pomanjkljivosti, kot so neustrezni postopki za upravljanje dostopov, pomanjkljiva dokumentacija ali nejasno določene odgovornosti. Čeprav taka tveganja niso tehnične narave, lahko pomembno vplivajo na varnost informacij, saj ustvarjajo neurejene in nenadzorovane postopke pri delu z digitalnimi sistemi (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Vrste groženj so tako povezane z delovanjem opreme, uporabniškimi napakami, zlonamernimi poskusi in organizacijskimi pomanjkljivostmi. Poznavanje teh skupin je pomembno za nadaljnje načrtovanje ukrepov, ki zmanjšujejo vpliv groženj na informacijske sisteme (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

2.5.2 Preventivni in korektivni ukrepi

Preventivni in korektivni ukrepi predstavljajo osrednji del upravljanja kibernetske varnosti. Namen preventivnih ukrepov je zmanjšati verjetnost, da bi prišlo do napak, zlorab ali motenj v delovanju informacijskih sistemov, medtem ko so korektivni ukrepi namenjeni odpravi posledic, ko se incident že zgodi. Učinkovito varnostno okolje je vedno kombinacija obeh pristopov, saj niti preventivni ukrepi ne morejo popolnoma izključiti tveganj, niti korektivni ukrepi ne morejo nadomestiti pomanjkljive preventive (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Med najpogostejše preventivne ukrepe spada dosledno upravljanje uporabniških pravic. Uporabniki imajo dostop samo do tistih virov, ki jih potrebujejo za svoje delo, kar zmanjša možnost nenamernih napak ali nepooblaščenega dostopa. Poleg tega se kot preventivni ukrep pogosto uporablja večfaktorska avtentikacija, ki omejuje možnost zlorabe prijavnih podatkov. Pomembno je tudi redno posodabljanje programske opreme in operacijskih sistemov, saj posodobitve odpravljajo ranljivosti, ki bi lahko omogočile dostop ali manipulacijo podatkov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Preventivni ukrepi vključujejo tudi organizacijske postopke, kot so jasno določene politike ravnanja z gesli, postopki prijave incidentov in redno ozaveščanje uporabnikov. Številni varnostni incidenti nastanejo zaradi nepozornosti ali nepoznavanja pravil, zato lahko izobraževanje in ustrezno načrtovane delovne prakse pomembno zmanjšajo tveganje. Med preventivne ukrepe spada tudi segmentacija omrežij, ki ločuje posamezne dele informacijskega sistema in tako preprečuje širjenje incidentov iz enega dela omrežja na drugega (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Korektivni ukrepi so usmerjeni v to, da se posledice incidentov čim hitreje odpravijo in da se povrne normalno delovanje sistema. Sem spadajo postopki za obnovo podatkov iz varnostnih kopij, sledenje spremembam v sistemih ter analiza vzroka, zaradi katerega je prišlo do incidenta. Korektivni ukrepi vključujejo tudi tehnično podporo v primeru okvar strojne opreme ter izvedbo dodatnih preverb, kadar je sum, da je prišlo do nepooblaščenega dostopa ali izgube podatkov (Priročnik kibernetske varnosti, 2025).

Razlikovanje med preventivnimi in korektivnimi ukrepi pomaga organizacijam vzpostaviti jasen sistem upravljanja varnosti. Preventiva zmanjšuje verjetnost težav, korektiva pa omejuje vpliv incidentov na delovanje sistemov in omogoča hitrejše okrevanje po napaki. Učinkovito upravljanje teh ukrepov je pomembno zlasti v okoljih, kjer se obdelujejo podatki z večjo občutljivostjo, saj lahko motnje v delovanju ali izgube podatkov neposredno vplivajo na zanesljivost informacij in potek dela (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

2.5.3 Vloga avtentikacije, šifriranja in segmentacije omrežij

Avtentikacija, šifriranje in segmentacija omrežij predstavljajo temeljne mehanizme za vzpostavljanje nadzora nad informacijskimi sistemi. Njihov namen je zagotoviti, da do podatkov dostopajo le upravičeni uporabniki, da so podatki varno prenašani med posameznimi

deli sistema ter da je omrežno okolje zasnovano tako, da morebitne napake ali incidenti ne vplivajo na delovanje celotnega sistema. Ti mehanizmi se uporabljajo v vseh okoljih, kjer se obdelujejo digitalne informacije, saj omogočajo nadzor nad dostopom in zmanjšujejo možnost nenadzorovanih sprememb, posegov ali izpadov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Avtentikacija je osnovni postopek, s katerim se preveri identiteta uporabnika ali naprave pred dodelitvijo dostopa. Najpogosteje se uporablja kombinacija uporabniškega imena in gesla, vendar se zaradi omejene zanesljivosti gesel v praksi vse bolj uveljavlja večfaktorska avtentikacija. Ta združuje različne načine preverjanja, npr. geslo, mobilno potrjevanje ali uporabo strojnega žetona. Namen avtentikacije je vzpostaviti zanesljiv način identifikacije, ki zmanjšuje možnost, da bi kdo nepooblaščen pridobil dostop zaradi uganjenih ali prestreženih poverilnic. Avtentikacija sama ne določa, kaj uporabnik lahko počne v sistemu; to določa avtorizacija, ki je povezana, vendar samostojna funkcija (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Šifriranje je mehanizem, ki omogoča zaščito podatkov pred nepooblaščenim dostopom med prenosom ali shranjevanjem. Pri šifriranju med prenosom se podatki pretvorijo tako, da so za zunanjega opazovalca neberljivi, tudi če bi bili prestreženi med komunikacijo. To je pomembno pri uporabi omrežnih povezav, še posebej pri tistih, kjer komunikacija poteka prek javnih ali deljenih omrežij. Pri šifriranju podatkov v mirovanju se zaščita izvaja neposredno na shranjevalnih napravah ali strežnikih, kar preprečuje, da bi fizični dostop do opreme omogočil vpogled v vsebino podatkov. Šifriranje se uporablja tudi kot dodaten sloj zaščite pri oblačnih storitvah, saj omogoča, da so podatki varovani tudi v primeru, ko se nahajajo zunaj organizacijskega omrežja (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Segmentacija omrežij predstavlja način organizacije omrežnega okolja, pri katerem se celotno omrežje razdeli na več manjših, med seboj ločenih delov. Namen segmentacije je, da se sistem razčleni na logične enote, ki imajo omejeno medsebojno povezljivost. Takšna zasnova bistveno zmanjša tveganje, da bi se morebitna zloraba ali napaka razširila na vse sisteme. Segmentacija je uporabna v primerih, ko se v organizaciji uporabljajo različne aplikacije ali sistemi, ki ne potrebujejo neposrednega stika drug z drugim. S tem se dodatno izboljša pregled nad dostopi, saj je mogoče jasno določiti, kateri uporabniki imajo dostop do posameznih delov sistema (Ivarnost.si, n.d.).

Skupna uporaba avtentikacije, šifriranja in segmentacije omogoča vzpostavitev večslojnega pristopa k informacijski varnosti. Vsak izmed teh mehanizmov ima svojo vlogo: avtentikacija določa identiteto in preprečuje nepooblaščen dostop, šifriranje varuje vsebino podatkov med prenosom in shranjevanjem, segmentacija pa zmanjšuje učinek morebitnih incidentov in preprečuje širjenje napak. Z uvedbo teh ukrepov organizacija pridobi jasnejši pregled nad delovanjem sistemov, zmanjša možnost nenadzorovanih posegov in poveča odpornost informacijskega okolja (Ivarnost.si, n.d.).

Učinkovitost teh pristopov je odvisna tudi od pravilnega upravljanja in rednega vzdrževanja. Napačne nastavitve pri avtentikaciji, nepravilno upravljanje šifrirnih ključev ali neustrezno načrtovana segmentacija lahko zmanjšajo učinek varnostnih ukrepov ali celo povzročijo nove ranljivosti. Zato se organizacije pogosto odločajo za redno preverjanje nastavitev in testiranje delovanja varnostnih mehanizmov, da se zagotovi njihova zanesljivost v vsakodnevnem delovanju (Ivarnost.si, n.d.).

2.5.4 Sodobni trendi v kibernetski varnosti

Sodobni razvoj informacijskih sistemov prinaša nove možnosti, hkrati pa ustvarja dodatne zahteve za njihovo zaščito. Zaradi vedno večje povezljivosti, uporabe oblačnih storitev ter razširjenosti mobilnih naprav se varnostni pristopi spreminjajo in dopolnjujejo. Trendi v kibernetski varnosti odražajo tehnološki napredek ter potrebo po boljšem nadzoru nad podatki in dostopi v okoljih, kjer se informacije nahajajo na različnih lokacijah in platformah (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Eden izrazitejših trendov je uvedba načela »ničelnega zaupanja« (zero trust). Ta pristop predpostavlja, da noben uporabnik ali naprava ne sme imeti dostopa do sistema brez preverjanja, ne glede na to, ali se nahaja znotraj ali zunaj organizacijskega omrežja. Zero trust tako nadomešča tradicionalne modele, ki so predvidevali večjo stopnjo zaupanja notranjim uporabnikom. Koncept temelji na razdelitvi sistema na manjše enote, stalnem preverjanju dostopov in omejevanju pravic glede na dejanske potrebe (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Pomemben trend predstavlja tudi vedno širša uporaba avtomatiziranih orodij za zaznavanje in odzivanje na varnostne incidente. Sistemi za spremljanje omrežja in strežnikov omogočajo odkrivanje neobičajnih vzorcev delovanja, ki lahko nakazujejo tehnične napake ali poskuse zlorab. Takšni sistemi pogosto vključujejo analizo podatkov in prepoznavanje odstopanj, kar omogoča hitrejši odziv na nepredvidene dogodke. Avtomatizirani postopki ne nadomeščajo varnostnih pravil, temveč dopolnjujejo obstoječe pristope in izboljšujejo pregled nad delovanjem sistemov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Z vse večjo uporabo oblačnih storitev se pojavlja tudi potreba po varnostnih pristopih, ki so prilagojeni deljenim okoljem. Pri tem je pomembno razumevanje, kako ponudniki oblačnih storitev obravnavajo varovanje podatkov, kako se izvajajo posodobitve ter katera orodja so na voljo za nadzor nad dostopom. Posledično se razvijajo rešitve, ki omogočajo večjo preglednost nad tem, kako se podatki prenašajo, shranjujejo in obdelujejo v oblačnih okoljih (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Varnostni trendi vključujejo tudi poudarek na zaščiti identitet in uporabniških računov. Ker številne storitve omogočajo dostop z različnih naprav in lokacij, postaja upravljanje identitet pomemben del varnostne strategije. Uporabljajo se sistemi, ki omogočajo pregled nad tem, kdaj in od kod uporabniki dostopajo do podatkov, ter orodja, ki obveščajo o nenavadnih prijavah ali spremembah v vedenju uporabnikov (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

Skupaj ti trendi kažejo na premik k bolj razdeljenim, prilagodljivim in preglednim varnostnim pristopom. Razvoj varnostnih mehanizmov poteka v smeri večjega nadzora nad dostopi, boljšega upravljanja identitet ter uporabe orodij, ki podpirajo hitro zaznavanje in odzivanje na nepravilnosti v delovanju informacijskih sistemov. Tak pristop omogoča stabilnejše delovanje ter zmanjša možnost, da bi incidenti vplivali na zanesljivost podatkov ali potek dela (URAD VLADE REPUBLIKE SLOVENIJE, 2025).

3. REGULATIVNA IZHODIŠČA

3.1 GDPR in varovanje osebnih podatkov

Varstvo osebnih podatkov v Evropski uniji ureja splošna uredba o varstvu podatkov (GDPR), ki določa pravila za zbiranje, obdelavo, hrambo in prenos osebnih podatkov ter zagotavlja enotno raven varstva pravic posameznikov v vseh državah članicah Evropske unije (Evropska unija, 2016). Namen uredbe je zagotoviti, da organizacije osebne podatke obdelujejo na pregleden, zakonit in nadzorovan način ter posameznikom omogočajo učinkovit nadzor nad njihovimi podatki.

GDPR opredeljuje osebne podatke kot vsak podatek, ki se nanaša na določljivo fizično osebo, ter določa obveznosti upravljavcev in obdelovalcev osebnih podatkov. Obdelava osebnih podatkov mora temeljiti na načelih zakonitosti, poštenosti in preglednosti, omejitve namena, najmanjšega obsega podatkov, točnosti, omejitve shranjevanja ter zagotavljanja integritete in zaupnosti (Evropska unija, 2016). Organizacije morajo posameznike jasno obvestiti o namenu obdelave, obdobju hrambe ter o tem, komu se lahko podatki razkrijejo.

Poseben poudarek uredba namenja uvedbi ustreznih tehničnih in organizacijskih ukrepov, s katerimi se zagotavlja varna obdelava osebnih podatkov. Ti ukrepi vključujejo nadzor nad dostopi, varno ravnanje z gesli, zaščito dokumentacije ter vzpostavitev postopkov za zaznavanje in prijavo kršitev varnosti osebnih podatkov. GDPR določa tudi obveznost vodenja evidenc dejavnosti obdelave ter obveznost obveščanja nadzornega organa in prizadetih posameznikov v primeru hujših kršitev varnosti podatkov (Evropska unija, 2016).

Uredba ureja tudi prenos osebnih podatkov zunaj Evropske unije, ki je dovoljen le v primerih, ko država prejemnica zagotavlja ustrezno raven varstva osebnih podatkov ali kadar so vzpostavljeni dodatni zaščitni mehanizmi, kot so standardne pogodbene klavzule (Evropska unija, 2016).

V okoljih, kjer se izvajajo raziskovalni postopki, laboratorijsko delo ali obdelava dokumentacije, se lahko pojavljajo osebni podatki donatorjev, pacientov ali sodelujočih posameznikov. Zato morajo organizacije zagotoviti, da so postopki obdelave osebnih podatkov skladni z določbami GDPR ter da je dostop do teh podatkov ustrezno omejen, nadzorovan in sledljiv (Evropska unija, 2016).

3.2 ISO/IEC 27001 in informacijska varnost

ISO/IEC 27001 je mednarodni standard, ki določa zahteve za vzpostavitev, upravljanje in izboljševanje sistema upravljanja informacijske varnosti (ISMS). Standard predstavlja strukturiran okvir, ki organizacijam pomaga obvladovati tveganja, povezana s shranjevanjem, prenosom in uporabo informacij (TecnoDigital, 2025).

Temelj standarda je vzpostavitev ISMS, ki vključuje politike, postopke in nadzorne mehanizme za zaščito informacij. Standard ne predpisuje, katere tehnologije mora organizacija uporabljati, temveč opredeljuje, da mora biti upravljanje informacijske varnosti načrtno, dokumentirano in usmerjeno v zmanjševanje tveganj. Organizacije morajo identificirati informacije, oceniti možne grožnje in določiti ukrepe, ki zmanjšujejo verjetnost incidentov ter njihov vpliv (TecnoDigital, 2025).

ISO/IEC 27001 se opira na model nenehnega izboljševanja »Plan–Do–Check–Act« (PDCA). V fazi načrtovanja organizacija določi varnostne cilje in postopke. V fazi izvajanja vzpostavi varnostne kontrole in procese. V fazi preverjanja ocenjuje učinkovitost obstoječih ukrepov, medtem ko faza ukrepanja vključuje izboljšave in prilagoditve glede na nove potrebe ali ugotovljene nepravilnosti (Ihonvbere, 2024).

Standard poudarja tudi pomen jasne razdelitve odgovornosti, upravljanja dostopov, spremljanja delovanja informacijskih sistemov ter dokumentiranja postopkov. Vsebuje priporočila za vzpostavitev nadzorovanega okolja, v katerem so procesi obdelave podatkov sledljivi, revizijsko podprti in zaščiteni pred motnjami (TecnoDigital, 2025).

Ker ISO/IEC 27001 obravnava celovit pristop k upravljanju informacijske varnosti, pogosto dopolnjuje zakonske zahteve, kot je GDPR. Organizacije ga lahko uporabljajo za krepitev svojih internih postopkov ter za zagotovitev, da so informacije zaščitene pred izgubo, nepooblaščenimi dostopi ali tehničnimi pomanjkljivostmi (TecnoDigital, 2025).

3.3 Zahteve za ravnanje z laboratorijskimi podatki

Laboratorijski podatki vključujejo rezultate meritev, zapisnike poskusov, instrumentne izpise, slikovne podatke, postopke, poročila in drugo dokumentacijo, ki nastane med raziskovalnim ali analitičnim delom. Podatki imajo ključno vlogo pri ponovljivosti rezultatov, dokazovanju skladnosti postopkov ter preverjanju poteka eksperimentov, zato morajo biti pri njihovem

upravljanju uporabljeni tehnični in organizacijski postopki, ki zagotavljajo sledljivost, celovitost in preglednost informacij (OECD, 2021).

Pri ravnanju z laboratorijskimi podatki se pogosto uporabljajo načela dobre dokumentacijske prakse, med katerimi so uveljavljena načela ALCOA+. Ta določajo, da morajo biti podatki pripisljivi, čitljivi, sočasno zapisani, izvirni in točni, razširjena različica pa vključuje tudi zahteve glede celovitosti, konsistentnosti, trajne dostopnosti in povezljivosti podatkov (OECD, 2021). Takšna načela omogočajo enoten pristop k dokumentiranju in arhiviranju podatkov ter prispevajo k njihovi verodostojnosti skozi celoten življenjski cikel (OECD, 2021).

Zaradi vse pogostejše uporabe digitalnih sistemov v laboratorijih je pomembno, da informacijska infrastruktura omogoča ustrezno sledljivost podatkov. To vključuje uporabo revizijskih sledi, ki beležijo spremembe v zapisih, ter nadzor dostopa, s katerim se zagotavlja, da podatke urejajo izključno pooblaščene osebe. Digitalni sistemi morajo omogočati rekonstrukcijo poteka eksperimenta, vključno z datumom in časom vnosa ter identifikacijo odgovornih oseb (OECD, 2021).

Pomemben vidik ravnanja z laboratorijskimi podatki je tudi dosledno upravljanje različic dokumentov in podatkovnih datotek. Takšen pristop omogoča shranjevanje prejšnjih različic ter jasno označevanje veljavnih zapisov, s čimer se zmanjšuje tveganje nenamernih sprememb ali izgube podatkov (ALCOA+ Data Integrity, 2025). Organizacije morajo hkrati vzpostaviti postopke za varnostno kopiranje in arhiviranje, saj periodične varnostne kopije omogočajo obnovo podatkov v primeru tehničnih napak ali napak pri delu (OECD, 2021).

Omejevanje dostopa do laboratorijskih podatkov na podlagi uporabniških vlog predstavlja dodatni mehanizem za zaščito informacij. Takšen nadzor zmanjšuje tveganje nepooblaščenih sprememb ter varuje občutljive podatke, ki se lahko pojavljajo v laboratorijski dokumentaciji (OECD, n.d.). Zahteve za ravnanje z laboratorijskimi podatki tako vključujejo natančno dokumentiranje, sledljivost postopkov, nadzor dostopa ter ustrezno arhiviranje, kar omogoča dolgoročno zanesljivost in ponovljivost laboratorijskega dela (OECD, 2021).

3.4 Regulativa povezana z delom z biološkimi materiali

Ravnanje z biološkimi materiali je v raziskovalnem okolju urejeno z etičnimi in pravnimi zahtevami, ki določajo pogoje za zbiranje, uporabo in dokumentiranje vzorcev, pri čemer je ključno spoštovanje pravic posameznikov ter zagotavljanje preglednosti in sledljivosti postopkov raziskovalnega dela (Council of Europe, 2012). Namen teh pravil je zaščititi pravice

posameznikov in zagotoviti, da je celoten postopek obravnave materiala pregleden in ustrezno evidentiran.

Pri uporabi vzorcev človeškega izvora je bistveno, da so postopki jasno opredeljeni in da je uporaba materiala v skladu z namenom, za katerega je bila dana privolitev. Privolitev mora biti informirana, kar pomeni, da mora posameznik predhodno razumeti, kako bo njegov biološki material uporabljen, kateri postopki bodo izvedeni ter pod kakšnimi pogoji bo potekalo shranjevanje in analiza materiala (Council of Europe, 2012).

Pri raziskavah, ki vključujejo biološke materiale, je običajno potrebna odobritev pristojnega etičnega odbora. Ta presoja raziskovalni namen, uporabljene metode, morebitna tveganja in načrtovane postopke ter preverja, ali je ravnanje z vzorci ustrezno utemeljeno in v skladu z etičnimi načeli ter veljavnimi standardi (Council of Europe, 2012).

Biološki materiali so pogosto povezani tudi z občutljivimi podatki o posameznikih, kot so zdravstveni ali genetski podatki. Zaradi tega je pomembno, da informacijski sistemi, ki podpirajo delo v laboratoriju, omogočajo nadzorovan dostop, ustrezno ločevanje podatkov ter zaščito dokumentacije, ki spremlja vzorce. Informacijski zapisi morajo biti organizirani tako, da je jasno razvidno, kdaj je bil material sprejet, kdo je z njim delal in kateri postopki so bili izvedeni, saj je takšna sledljivost nujna za zagotavljanje preglednosti in možnosti rekonstrukcije raziskovalnega dela (Council of Europe, 2012).

Informacijski sistemi morajo podpirati enolično označevanje vzorcev ter hranjenje podatkov, ki so povezani z raziskovalnimi postopki. Pomembno je, da se podatki o vzorcih in postopkih shranjujejo na način, ki omogoča kasnejše preverjanje, ne da bi bil ogrožen identitetni podatek posameznika. V praksi to pogosto pomeni uporabo psevdonimizacije ali ločevanja identifikacijskih podatkov od raziskovalnih podatkov, tako da so osebni podatki dostopni le tam, kjer je to nujno (Council of Europe, 2012).

Regulativa tako vpliva na organizacijo laboratorijskega dela in na informacijsko infrastrukturo, ki mora omogočati ustrezno dokumentiranje, nadzor nad dostopi ter varno hrambo informacij. Učinkovit informacijski sistem podpira skladnost z etičnimi zahtevami, saj omogoča, da so vsi postopki z biološkimi materiali pregledni, pravilno evidentirani ter izvedeni v skladu z določenimi pravili in smernicami (Council of Europe, 2012).

4. OPIS PODJETJA IN KONTEKSTA DELA

4.1 Področje dejavnosti podjetja

Podjetje deluje na področju raziskav in razvoja tehnologij za delo s celicami. Ključni del dejavnosti predstavljajo razvoj in optimizacija metod za izolacijo celičnih populacij, njihovo procesiranje, aktivacijo ter druge postopke, ki podpirajo uporabo celic v biotehnoloških in terapevtskih aplikacijah. Delo vključuje načrtovanje eksperimentov, preizkušanje različnih pristopov ter sistematično izboljševanje procesov na podlagi analiz in meritev.

Zaradi izrazito raziskovalne narave dela pri vsakem postopku nastajajo podatki, ki imajo pomembno vlogo pri nadaljnjem razvoju tehnologij. Ti podatki predstavljajo temelj za oceno uspešnosti posameznih metod, primerjavo rezultatov in sprejemanje razvojnih odločitev. Zato je ključnega pomena, da so shranjevanje, organizacija in zaščita podatkov urejeni na način, ki zagotavlja njihovo sledljivost, celovitost in dolgoročno dostopnost. Raziskovalno okolje zato zahteva stabilno informacijsko infrastrukturo ter jasno definirane postopke za upravljanje podatkov, ki nastajajo pri vsakodnevnem delu.

4.2 Značilnosti laboratorijskih postopkov

Laboratorijsko delo v podjetju temelji na izvajanju raziskovalnih in razvojnih postopkov, pri katerih se preizkušajo različne metode za izolacijo, ločevanje in obdelavo celic. Postopki vključujejo kombinacijo mehanskih, biokemijskih in analitskih pristopov, ki omogočajo pridobivanje podatkov o učinkovitosti posameznih metod ter o lastnostih pripravljenih celičnih populacij. Ker so postopki pogosto eksperimentalni in iterativni, je pomembno natančno dokumentiranje izvedenih korakov in spremljanje sprememb, ki nastanejo med optimizacijo (OECD, 2021)

Del raziskovalnega dela vključuje uporabo laboratorijske opreme, kot so mikroskopi, merilni sistemi in druge analitske naprave, ki ustvarjajo podatke v različnih oblikah. Ti podatki zajemajo slikovne zapise, vrednosti meritev, instrumentne izpise ter rezultate analiz, ki se kasneje uporabljajo pri interpretaciji, primerjavi in načrtovanju nadaljnjih poskusov. Pomemben del laboratorijskih postopkov predstavljajo tudi standardizirani protokoli, ki omogočajo ponovljivost rezultatov in doslednost pri izvajanju posameznih metod (OECD, 2021).

Zaradi narave raziskovalnega procesa, ki vključuje prilagajanje postopkov, uvajanje novih pristopov in medsebojno primerjavo rezultatov, je treba zagotoviti jasno sledljivost ter ustrezno upravljanje dokumentacije. Dosledno beleženje postopkov, organizacija podatkov in nadzor nad dostopi omogočajo stabilen raziskovalni potek ter zmanjšujejo možnost napak ali nedoslednosti, ki bi lahko vplivale na rezultate raziskav (OECD, 2021).

4.3 Vrste podatkov, ki nastajajo pri delu

Pri izvajanju raziskovalnih in laboratorijskih postopkov nastajajo različne vrste podatkov, ki se med seboj razlikujejo glede na namen, obliko in kritičnost. Najobsežnejšo skupino predstavljajo raziskovalni zapisi, ki dokumentirajo potek eksperimentov, uporabljene postopke, izmerjene vrednosti in opažanja. Ti zapisi omogočajo ponovljivost postopkov ter zagotavljajo pregled nad razvojnimi koraki, ki vodijo do novih ali izboljšanih metod (Neng W., 2025).

Pomemben del podatkov predstavljajo poročila kakovosti (QC), ki odražajo skladnost izvedenih postopkov z internimi smernicami in preverjajo ustreznost posameznih korakov v raziskovalnem procesu. QC poročila vključujejo meritve, kontrole, validacije in preglede, ki so potrebni za potrditev zanesljivosti rezultatov (OECD, 2021).

V laboratorijskem okolju nastaja tudi tehnična in vizualna dokumentacija, med katero spadajo mikroskopske slike, instrumentni izpisi, numerični podatki meritev ter druge analitske datoteke. Ti podatki se uporabljajo pri interpretaciji rezultatov, primerjavi med postopki ter pri dokumentiranju sprememb, ki nastanejo med optimizacijo metod (OECD, 2021).

Poleg raziskovalne in analitske dokumentacije v podjetju nastajajo še pravna in administrativna gradiva, kot so pogodbe, razvojni dokumenti, interne smernice, evidence postopkov ter podatki, povezani z intelektualno lastnino, vključno s patentnimi prijavami ali tehničnimi opisi rešitev. Zaradi heterogene narave podatkov je potrebno jasno razmejevanje med vrstami dokumentacije ter ustrezna organizacija shranjevanja, ki omogoča preglednost in nadzor nad celotnim podatkovnim tokom (OECD, 2021).

4.4 Obstoječa IT-infrastruktura

Obstoječa IT-infrastruktura podjetja je vzpostavljena tako, da podpira administrativne procese, laboratorijsko delo ter varno obdelavo raziskovalnih podatkov. Omrežna arhitektura je organizirana hierarhično in omogoča jasno ločitev posameznih funkcionalnih sklopov, kar pripomore k preglednosti, stabilnosti ter varnemu upravljanju podatkovnih tokov.

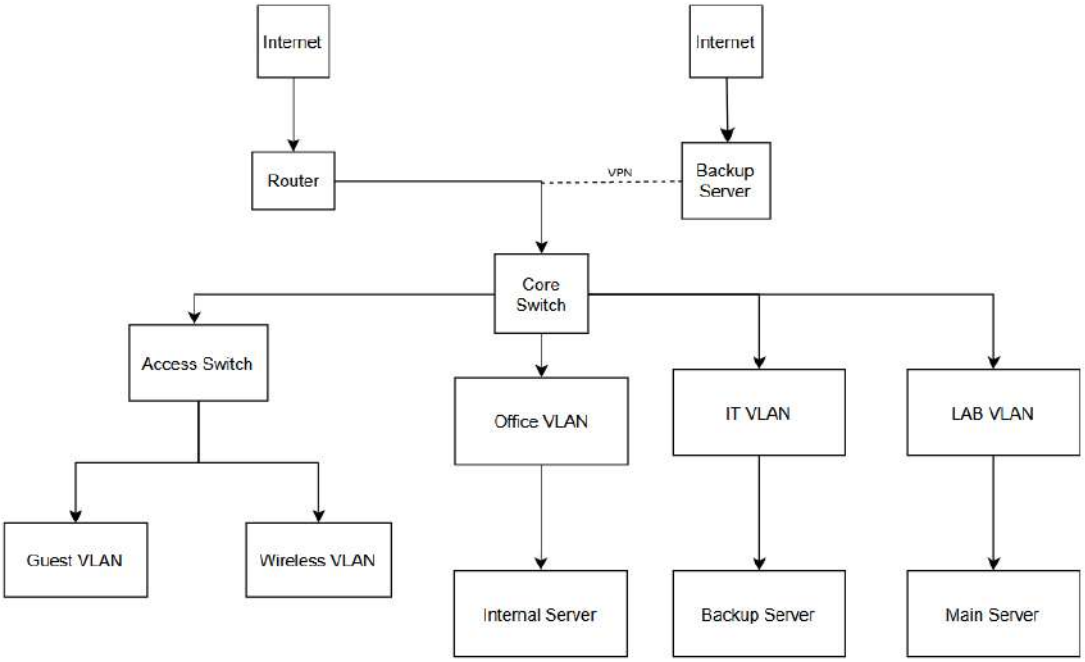
Dostop do interneta poteka prek usmerjevalnika, ki deluje kot glavni prehod v omrežje ter skrbi za osnovne varnostne mehanizme. Usmerjevalnik je povezan s centralnim stikalom (core switch), ki predstavlja osrednje vozlišče omrežja in omogoča razporeditev prometa na posamezne segmente. Od centralnega stikala se omrežje razdeli na več funkcionalnih sklopov, organiziranih glede na delovne procese v podjetju.

Pisarniški del omrežja je povezan prek Office VLAN-a, ki omogoča dostop do administrativnih storitev in interne dokumentacije. Laboratorijsko okolje je ločeno v LAB VLAN, kjer se nahajajo naprave, računalniki in strežniki, ki so vključeni v raziskovalne postopke. V tem delu omrežja je nameščen glavni strežnik, ki omogoča hrambo eksperimentalnih podatkov, analiz in pripadajoče dokumentacije. Poseben segment predstavlja IT VLAN, ki je namenjen vzdrževanju notranje infrastrukture ter vključuje lokalni backup strežnik.

Vzpostavljen je tudi ločen del omrežja za brezžične in gostujoče uporabnike, ki je oddaljen od občutljivih podatkovnih virov. Wireless in Guest VLAN sta povezana prek samostojnega dostopnega stikala, kar preprečuje nenadzorovan dostop do notranjih podatkovnih okolij ter varuje celovitost raziskovalnih informacij.

Poleg lokalnega backup strežnika je v sistemu vzpostavljen tudi dodatni oddaljeni strežnik, ki je povezan prek varne povezave VPN. Ta rešitev omogoča geografsko ločeno varnostno kopiranje in tako dodatno ščiti podatke v primeru okvare opreme, nepredvidenih dogodkov ali izgube dostopa na primarni lokaciji.

Fizična infrastruktura vključuje nabor dostopnih stikal, ki povezujejo laboratorijske prostore, pisarne in nadzorne točke. Strežniki so nameščeni na dostopnem nivoju, kar omogoča preprosto integracijo z delovno opremo ter zagotavlja nemoten prenos podatkov v realnem času. Jasna segmentacija omrežja ter redundančne rešitve zagotavljajo visoko stopnjo zanesljivosti in omogočajo stabilno podporo raziskovalnim postopkom.



Slika 4.4-1: Infrastruktura omrežja podjetja.

Vir: Lastna priprava

4.5 Trenutni način shranjevanja podatkov

Trenutni sistem shranjevanja podatkov v podjetju temelji na centralizirani uporabi lokalnega strežnika (NAS), ki deluje kot glavno mesto za hrambo raziskovalnih, laboratorijskih in administrativnih podatkov. Strežnik omogoča sočasen dostop več uporabnikov ter zagotavlja stabilno okolje za organizacijo dokumentacije, ki nastaja pri eksperimentih, analizah ter vsakodnevnih delovnih procesih.

V podjetju se podatki shranjujejo pretežno lokalno. Eksperimentalni zapisi, poročila QC, mikroskopske slike, instrumentni izpisi ter ostala raziskovalna dokumentacija se ustvarijo na posameznih delovnih postajah in laboratorijskih računalnikih, nato pa se ročno prenesejo na strežnik. Tak način omogoča raziskovalcu pregled nad kakovostjo podatkov pred arhiviranjem, vendar vključuje tudi določeno stopnjo odvisnosti od doslednega izvajanja postopka s strani uporabnika.

Organizacija podatkov na strežniku temelji na strukturirani mapni zasnovi, ki omogoča jasen pregled nad raziskovalnimi projekti, protokoli, pravno dokumentacijo ter instrumentnimi datotekami. Mapna struktura je oblikovana tako, da omogoča sledljivost informacij ter enostavno iskanje dokumentov glede na fazo projekta ali vrsto analize.

Dostop do podatkov je urejen prek omrežnih dovoljenj in ločenih segmentov. Uporabniki imajo pravice le do tistih vsebin, ki so potrebne za njihovo delo, kar zmanjšuje možnost neželenih sprememb ali nenadzorovanega dostopa. Administrativno osebje dostopa do Office VLAN-a, medtem ko raziskovalna ekipa dostopa do podatkov prek LAB VLAN-a. Podatki v IT VLAN-u so dostopni izključno osebam, odgovornim za vzdrževanje infrastrukture.

Za zagotavljanje celovitosti podatkov se redno izvajajo varnostne kopije na lokalni backup strežnik. Poleg tega je vzpostavljeno tudi oddaljeno varnostno kopiranje prek varne povezave VPN, ki omogoča geografsko ločeno shranjevanje podatkov. To predstavlja dodatno zaščito v primeru okvar strojne opreme, izgube prostora ali morebitnih varnostnih incidentov.

Takšen sistem, ki združuje centralizirano lokalno shranjevanje, strukturirano organizacijo podatkov, nadzorovan dostop in večstopenjsko varnostno kopiranje, zagotavlja stabilno podporo raziskovalnim procesom ter omogoča varno upravljanje podatkov skozi celoten življenjski cikel raziskovalnega dela.

5. ANALIZA LOKALNEGA SHRANJEVANJA PODATKOV V PODJETJU

5.1 Strojna in programska infrastruktura

Lokalno shranjevanje podatkov v podjetju temelji na uporabi centralnega omrežnega strežnika (NAS), ki predstavlja glavni nosilec podatkovne infrastrukture. Strežnik je zasnovan kot primarna točka za hrambo raziskovalnih, laboratorijskih in administrativnih podatkov, pri čemer omogoča sočasni dostop več uporabnikov ter deluje kot osrednji repozitorij za podatke, ki nastajajo pri vsakodnevnem delu. Na strežnik so povezani tako pisarniški sistemi kot laboratorijska oprema, za katero je značilno, da ustvarja večje količine podatkov v različnih formatih.

V podjetju je vzpostavljen tudi ločen strežnik za varnostno kopiranje, ki se nahaja v drugi fizični lokaciji kot glavni strežnik. Takšna prostorska ločitev zmanjšuje tveganje izgube podatkov v primeru okvar, poškodb opreme ali nepredvidenih dogodkov v posameznem prostoru. Redno izvajanje varnostnega kopiranja tako predstavlja ključen del infrastrukture, saj zagotavlja obnovljivost podatkov in dodatno stopnjo zaščite v primeru napak v delovanju primarnega sistema.

Dostop do strežnikov in delovnih postaj omogoča lokalna omrežna infrastruktura, ki je zasnovana s pomočjo več medsebojno povezanih dostopnih stikal. Ta stikala povezujejo pisarniške in laboratorijske prostore ter omogočajo ločevanje posameznih delovnega okolij. S tem je zagotovljena večja preglednost pri obdelavi podatkov ter omejen dostop do občutljive dokumentacije. Laboratorijska oprema, računalniki v laboratorijih in pisarniške naprave so povezani na namenska stikala glede na delovno področje, kar omogoča jasen nadzor nad pretokom podatkov in zagotavlja stabilno komunikacijo z osrednjim strežnikom.

Programsko okolje, ki podpira lokalno shranjevanje podatkov, sestavljajo orodja, ki omogočajo pregled, urejanje in organizacijo podatkov. Med najpogosteje uporabljenimi so preglednice (Excel), besedilna orodja (Word), komunikacijski kanal (angl. Slack) ter sistema za organizacijo in filtriranje rezultatov (angl. Airtable). Ti programi ne služijo kot primarni prostor za shranjevanje podatkov, temveč kot podporna orodja, ki omogočajo analizo, pripravo dokumentacije ter jasen pregled nad potekom eksperimentov.

Takšna kombinacija strojne in programske opreme predstavlja stabilen temelj lokalnega shranjevanja podatkov ter omogoča učinkovito podporo raziskovalnemu in administrativnemu delu v podjetju. V naslednjih poglavjih bo podrobneje analizirano, kako se podatki organizirajo, varujejo in arhivirajo v okviru obstoječega sistema.

5.2 Organizacija podatkov na lokalnih sistemih

Organizacija podatkov na lokalnih sistemih v podjetju je zasnovana centralizirano in temelji na uporabi več strežnikov z jasno določenimi vlogami. Osrednji strežnik predstavlja glavno mesto za shranjevanje vseh raziskovalnih, laboratorijskih in administrativnih podatkov. Poleg glavnega strežnika je vzpostavljen ločen varnostni strežnik, ki služi kot varnostna kopija glavnega sistema, dodatni strežnik, namenjen oddaljenemu dostopu, ter poseben strežnik za pisarniško in administrativno delo. Takšna razdelitev omogoča večjo zanesljivost delovanja in boljšo organizacijo podatkovnega okolja.

Dostop do lokalnih strežnikov poteka preko omrežnih povezav, pri čemer se uporabniki na strežnik povežejo in uporabljajo skupne mape. Podatki se ne shranjujejo lokalno na delovnih računalnikih, temveč izključno na strežnikih, kar zmanjšuje tveganje izgube podatkov in omogoča centralni nadzor nad shranjevanjem. Vsi laboratorijski in pisarniški računalniki so tako namenjeni delu, končni podatki pa se sistematično hranijo na strežniški infrastrukturi.

Struktura map na glavnem strežniku je organizirana po vsebinskih sklopih. Posebna mapa je namenjena raziskovalnemu delu, znotraj katere so podatki nadalje razdeljeni po posameznih projektih. Vsak projekt ima svojo mapo, ki vsebuje podmape za rezultate eksperimentov, slikovno gradivo, analize in spremljajočo dokumentacijo. Takšna organizacija omogoča preglednost nad potekom raziskovalnega dela in olajša iskanje podatkov tudi za nazaj. Druge mape na strežniku so namenjene administrativnim, dokumentacijskim in razvojnim vsebinam ter so prav tako strukturirane glede na namen uporabe.

Način poimenovanja map in datotek temelji predvsem na dogovoru med zaposlenimi. V praksi se pogosto uporabljajo ključne besede, ki opisujejo vsebino eksperimenta ali projekta, kar omogoča hitrejše iskanje starejših podatkov in boljšo orientacijo v večji količini shranjenih informacij. Čeprav ta pristop zahteva določeno mero discipline uporabnikov, se je v praksi izkazal kot uporaben pri vsakodnevnem delu.

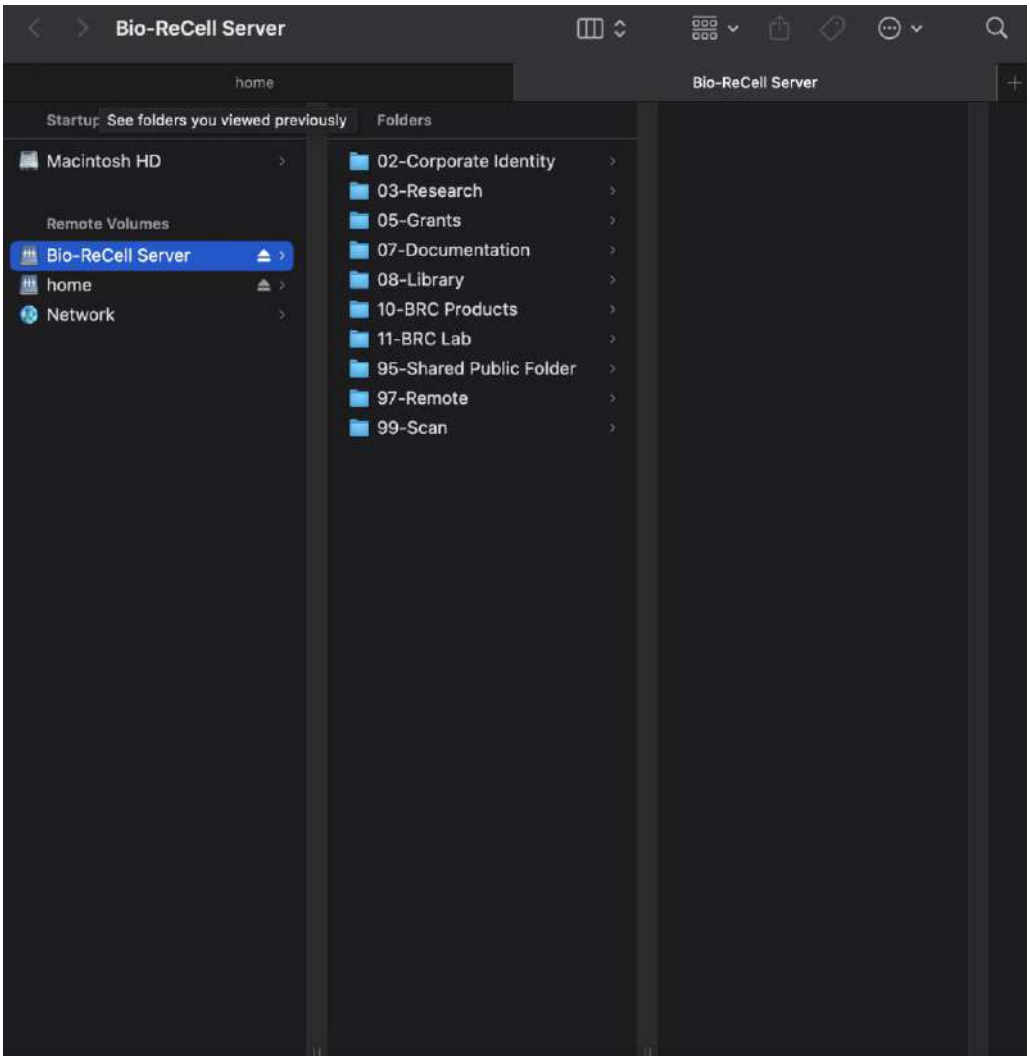
Dostop do podatkov je urejen preko uporabniških pravic, ki jih določa informacijska podpora podjetja. Zaposleni imajo omogočen dostop samo do tistih map, ki jih potrebujejo za

opravljanje svojega dela. Laboratorijsko osebje ima dostop do raziskovalnih in eksperimentalnih podatkov, administrativni uporabniki do pisarniških dokumentov, medtem ko so določene vsebine dostopne zgolj omejenemu krogu uporabnikov. Študenti in zunanji sodelavci imajo dostop močno omejen in ločen od ostalih podatkov, kar dodatno zmanjšuje tveganje nepooblaščenega dostopa.

Podatki se na strežnik shranjujejo takoj po zaključenem eksperimentu oziroma po opravljeni analizi. Pred shranjevanjem uporabniki preverijo pravilnost in popolnost podatkov ter jih ustrezno razporedijo v projektne mape. Takšen način dela zagotavlja, da so na strežniku shranjeni le urejeni in relevantni podatki ter da ni potrebe po dodatnem naknadnem urejanju.

Glavna prednost takšne organizacije podatkov je popoln nadzor nad informacijami, saj so vsi podatki shranjeni znotraj lastne infrastrukture podjetja. Ker podatki predstavljajo pomembno raziskovalno in razvojno vrednost, je takšen pristop za podjetje ustreznejši kot uporaba zunanjih storitev. Kljub temu organizacija podatkov zahteva doslednost zaposlenih, saj je kakovost shranjenih informacij v veliki meri odvisna od pravilnega shranjevanja in urejanja podatkov po zaključenem delu.

Opisana organizacija podatkov in način dostopa do lokalnih strežnikov je prikazana tudi na sliki, ki ponazarja povezovanje uporabnikov z osrednjim strežnikom ter pregled osnovne strukture map. Slika služi kot dopolnilo besedilu in omogoča lažjo predstavo dejanskega delovanja podatkovnega okolja v podjetju.



Slika 5.2.-1: Razporeditev map in organizacija v lokalnem omrežju podjetja.

Vir: Bio-Recell, d. o. o

5.3 Varnost lokalne infrastrukture

Varnost lokalne infrastrukture v podjetju je zasnovana celostno in vključuje fizične, omrežne ter organizacijske ukrepe. Namen takšne ureditve je zagotoviti stabilno delovanje informacijskih sistemov ter zaščito podatkov, ki predstavljajo pomembno raziskovalno in razvojno vrednost. Poseben poudarek je namenjen nadzoru dostopov in omejevanju izpostavljenosti zunanjim tveganjem.

Fizična varnost strežnikov je urejena z ločenimi in nadzorovanimi lokacijami. Glavni strežnik, na katerem so shranjeni ključni podatki podjetja, je nameščen v posebnem zaklenjenem prostoru. Fizični dostop do prostora ima informacijska podpora podjetja, ki razpolaga s ključi.

Strežnik za varnostne kopije je nameščen v prostoru informacijske podpore, pisarniški strežnik v ločenem prostoru, dodatni strežnik za oddaljene funkcionalnosti pa na drugi lokaciji. Prostori, v katerih se nahajajo strežniki, so ustrezno prezračevani, temperatura pa se spremlja, kar prispeva k zanesljivemu delovanju strojne opreme.

Omrežna varnost temelji predvsem na omejevanju dostopa do sistemov znotraj lokalnega omrežja. Večina strežnikov ni neposredno dostopna iz zunanjega omrežja, kar zmanjšuje tveganje nepooblaščenih dostopov. Za posebne potrebe je vzpostavljen ločen sistem, ki omogoča oddaljen dostop, pri čemer je ta ločen od glavnega strežniškega okolja. Požarni zid in druge varnostne funkcije so del omrežne opreme, omrežje pa je razdeljeno na več segmentov glede na namen uporabe, na primer laboratorijski in pisarniški del.

Dostop do informacijskih sistemov je urejen preko uporabniških računov. Vsak zaposleni ima dodeljen osebni uporabniški račun, ki ga ob vzpostavitvi delovnega okolja uredi informacijska podpora podjetja. Pravice dostopa do strežnikov in posameznih map se dodeljujejo glede na vlogo uporabnika in njegove delovne naloge. Določeni sistemi in mape so dostopni le omejenemu številu uporabnikov, dostop študentov in zunanjih sodelavcev pa je strogo omejen in ločen od drugih podatkov.

Varnost podatkov je zagotovljena z uporabo uporabniških dovoljenj in centraliziranim upravljanjem dostopov. Podatki se ne shranjujejo na lokalnih delovnih računalnikih, temveč izključno na strežnikih, kar omogoča boljši nadzor nad dostopi in zmanjšuje tveganje izgube podatkov. Informacijska podpora vodi pregled nad dodeljenimi dovoljenji z uporabo lastnih orodij in sistemov.

Operativna varnost temelji na stalni prisotnosti in odzivnosti informacijske podpore. V primeru tehničnih težav je omogočen hiter odziv, vključno z oddaljenim upravljanjem in ponovnim zagonom sistemov. Podjetje do sedaj ni imelo primerov izgube podatkov, občasne težave z delovanjem internetne povezave pa niso vplivale na varnost ali celovitost shranjenih informacij.

5.4 Postopki varnostnega kopiranja

Postopki varnostnega kopiranja v podjetju so zasnovani avtomatizirano in predstavljajo pomemben del zagotavljanja varnosti ter zanesljivosti podatkovnega okolja. Namen varnostnih kopij je zaščita podatkov pred izgubo zaradi tehničnih okvar, napak uporabnikov ali drugih nepredvidenih dogodkov. Sistem varnostnega kopiranja je prilagojen naravi raziskovalnega dela, kjer imajo podatki visoko vrednost in morajo biti dolgoročno ohranjeni.

Varnostne kopije se izvajajo samodejno in večkrat dnevno. Kopiranje zajema celoten strežniški sistem, kar pomeni, da so vključeni vsi podatki, shranjeni na glavnem strežniku. Tak pristop omogoča celovito zaščito podatkovnega okolja in zmanjšuje tveganje, da bi bili posamezni deli podatkov izpuščeni iz varnostnega kopiranja. Avtomatizacija postopkov zmanjšuje odvisnost od ročnih posegov in možnost človeških napak.

Podatki se shranjujejo na več ločenih lokacijah. Poleg glavnega strežnika je vzpostavljen poseben strežnik za varnostne kopije, dodatna kopija podatkov pa se hrani tudi na drugi fizični lokaciji. Takšna razporeditev zagotavlja dodatno zaščito v primeru izpada ali okvare na eni lokaciji ter povečuje zanesljivost celotnega sistema varnostnega kopiranja.

Za izvajanje in upravljanje varnostnih kopij se uporabljajo namenska programska orodja, ki so del informacijske infrastrukture podjetja. Informacijska podpora spremlja delovanje sistema varnostnega kopiranja ter nadzoruje uspešnost posameznih kopij. V primeru morebitnih nepravilnosti je omogočeno hitro ukrepanje, kar prispeva k stabilnosti delovanja informacijskih sistemov.

Dostop do varnostnih kopij je strogo omejen. Do sistemov za varnostno kopiranje ima dostop izključno informacijska podpora podjetja, kar preprečuje nepooblaščeno uporabo ali spreminjanje varnostnih kopij. Redni uporabniki nimajo neposrednega dostopa do teh sistemov, s čimer je dodatno zagotovljena varnost shranjenih podatkov.

Do sedaj v podjetju ni bilo potrebe po obnovi podatkov iz varnostnih kopij, saj ni prišlo do izgube podatkov. Kljub temu vzpostavljen sistem omogoča obnovo v primeru potrebe, pri čemer bi postopek izvedla informacijska podpora. Takšna ureditev zagotavlja, da je podjetje pripravljeno tudi na izredne situacije, čeprav se v praksi do sedaj še niso pojavile.

5.5 Prednosti in slabosti obstoječe rešitve

Obstoječa rešitev lokalnega shranjevanja podatkov v podjetju prinaša več pomembnih prednosti, zlasti z vidika nadzora nad podatki in podpore raziskovalnemu delu. Centralizirana strežniška infrastruktura omogoča, da so vsi ključni podatki shranjeni znotraj lastnega okolja podjetja, kar zmanjšuje odvisnost od zunanjih ponudnikov in povečuje zaupanje v varnost podatkov. Takšen pristop je posebej primeren za raziskovalno okolje, kjer imajo podatki visoko vrednost in predstavljajo pomemben del intelektualne lastnine.

Prednost obstoječe rešitve je tudi jasna organizacija podatkov in ločevanje vsebin glede na namen uporabe. Razdelitev podatkov po projektih, vsebinskih sklopih in uporabniških vlogah omogoča preglednost ter učinkovito vsakodnevno delo. Centralno upravljanje dostopov in uporabniških pravic dodatno prispeva k varnosti in zmanjšuje tveganje nepooblaščenega dostopa. Pomemben vidik predstavlja tudi vzpostavljen sistem varnostnega kopiranja, ki z več kopijami podatkov in ločenimi lokacijami zagotavlja visoko stopnjo zaščite pred izgubo podatkov.

Kljub številnim prednostim ima obstoječa rešitev tudi določene omejitve. Učinkovitost sistema je v veliki meri odvisna od discipline uporabnikov pri shranjevanju in urejanju podatkov. Ker poimenovanje map in datotek temelji predvsem na dogovoru med zaposlenimi, lahko ob pomanjkanju doslednosti pride do manjše preglednosti ali podvajanja vsebin. Poleg tega lokalna infrastruktura zahteva stalno vzdrževanje in aktivno vlogo informacijske podpore, kar pomeni dodatno organizacijsko in kadrovsko obremenitev.

Omejitev predstavlja tudi omejena prilagodljivost pri oddaljenem dostopu, saj je večina sistemov namenoma dostopna predvsem znotraj lokalnega omrežja. Takšna ureditev sicer povečuje varnost, vendar lahko v določenih primerih oteži delo na daljavo. Prav tako je treba dolgoročno razmišljati o nadgradnjah strojne in programske opreme, saj lokalna infrastruktura zahteva periodične investicije za ohranjanje zanesljivosti in zmogljivosti.

Na podlagi analize je mogoče ugotoviti, da obstoječa rešitev lokalnega shranjevanja podatkov dobro podpira potrebe podjetja in je ustrezno prilagojena raziskovalnemu okolju. Prednosti, povezane z nadzorom, varnostjo in preglednostjo, trenutno presegajo zaznane omejitve, kar utemeljuje uporabo lokalne infrastrukture kot osnovnega podatkovnega okolja.

6. ANALIZA OBLAČNEGA SHRANJEVANJA PODATKOV V PODJETJU

6.1 Podatki, shranjeni v oblačnem okolju

Oblačno shranjevanje podatkov v podjetju se uporablja kot podporno okolje za organizacijo dela in komunikacijo med zaposlenimi. V oblak se shranjujejo podatki, ki niso neposredno povezani z laboratorijskimi eksperimenti ali raziskovalnimi rezultati, temveč služijo predvsem koordinaciji, načrtovanju in sodelovanju znotraj podjetja.

V oblačnem okolju se hranijo komunikacijski podatki, kot so pogovori med zaposlenimi, zapiski in povzetki sestankov ter ideje za prihodnje aktivnosti in eksperimente. Poleg tega se v oblak shranjujejo urniki, sporedi dejavnosti in druge vsebine, povezane z organizacijo dela. Poseben del oblačnih storitev se uporablja tudi za marketinške vsebine, ki niso povezane z raziskovalnimi podatki podjetja.

Podatki, ki nastajajo pri izvajanju laboratorijskih eksperimentov, kot so eksperimentalni rezultati, protokoli, surovi podatki, analize in slikovno gradivo, se v oblak ne shranjujejo. Ti podatki so hranjeni izključno na lokalnih strežniških sistemih podjetja. Takšna ločitev omogoča jasno razmejitev med organizacijskimi in raziskovalnimi podatki ter zmanjšuje tveganje, da bi se občutljive informacije znašle v oblačnem okolju.

Oblačne storitve uporabljajo vsi zaposleni v podjetju. Dostop do teh storitev je omogočen izključno preko službenih uporabniških računov, pri čemer sta za prijavo potrebna službeni elektronski naslov in geslo. Dostop je omogočen iz službenih delovnih računalnikov ter iz mobilnih naprav zaposlenih, ki imajo nameščene ustrezne aplikacije za delo v oblaku.

Občutljivost podatkov, shranjenih v oblačnem okolju, je ocenjena kot srednja. Gre za podatke, ki so pomembni za organizacijo dela, vendar ne predstavljajo kritičnih raziskovalnih ali razvojnih informacij. V podjetju obstaja neformalni dogovor med zaposlenimi glede tega, katere vrste podatkov se smejo shranjevati v oblak in katere morajo ostati izključno na lokalnih sistemih.

Takšna uporaba oblačnega shranjevanja omogoča boljšo preglednost nad delovnimi procesi in učinkovitejšo komunikacijo, hkrati pa ohranja raziskovalne podatke znotraj lokalne infrastrukture podjetja.

6.2 Varnost oblačnega shranjevanja podatkov v podjetju

Varnost oblačnega shranjevanja podatkov v podjetju temelji predvsem na nadzoru dostopov, omejitvi vrst podatkov, ki se shranjujejo v oblak, ter na vlogi informacijske podpore pri upravljanju uporabniških pravic. Oblačne storitve se uporabljajo v omejenem obsegu in so namenjene predvsem komunikaciji ter organizaciji dela, kar vpliva tudi na način zagotavljanja njihove varnosti.

Dostop do oblačnih storitev je urejen preko uporabniških računov. Pri nekaterih storitvah ima vsak zaposleni svoj osebni uporabniški račun, pri drugih pa se uporabljajo skupni računi. V vseh primerih so gesla za oblačne storitve ločena od gesel, ki se uporabljajo za prijavo v lokalne informacijske sisteme. Dodatna zaščita pri prijavi je zagotovljena z uporabo potrditvenih kod, ki se pošiljajo na elektronski naslov, do katerega ima dostop izključno informacijska podpora podjetja.

Dostop do oblačnih storitev je omogočen iz službenih delovnih računalnikov ter iz mobilnih naprav zaposlenih, na katerih so nameščene ustrezne aplikacije. Dostop iz zasebnih računalnikov ni dovoljen, kar zmanjšuje tveganje nepooblaščenega dostopa in omogoča boljši nadzor nad uporabo oblačnih storitev. Takšna ureditev omejuje število potencialno tveganih dostopnih točk.

Nadzor nad uporabo oblačnih storitev izvaja informacijska podpora predvsem v primeru težav ali nepravilnosti. Evidenca dostopov in aktivnosti se hrani na lokalnih sistemih podjetja, kar omogoča dodatno sledljivost in pregled nad uporabo oblačnih orodij. V podjetju obstaja tudi jasen dogovor glede omejitev uporabe oblaka, pri čemer so zaposleni seznanjeni s tem, da se raziskovalni in eksperimentalni podatki ne shranjujejo v oblačne storitve.

6.3 Upravljanje dostopa v oblačnih sistemih

Upravljanje dostopa v oblačnih sistemih v podjetju temelji na kombinaciji uporabniških računov, dodeljevanja pravic in nadzora s strani informacijske podpore. Namen takšne ureditve je zagotoviti, da imajo zaposleni dostop le do vsebin, ki so relevantne za njihovo delo, ter preprečiti nepooblaščen dostop do oblačnih storitev.

Dostop do oblačnih storitev je omogočen preko službenih uporabniških računov. Pri nekaterih orodjih ima vsak zaposleni svoj osebni račun, pri drugih pa se uporabljajo skupni računi. Gesla za oblačne storitve so ločena od gesel za lokalne informacijske sisteme. Prijava je dodatno

zaščitena s potrditvenimi kodami, ki se pošiljajo na službeni elektronski naslov, do katerega ima dostop izključno informacijska podpora podjetja.

Pravice dostopa se ne dodeljujejo enotno vsem uporabnikom. Upravljanje pravic izvaja informacijska podpora oziroma pooblaščena oseba z administratorskimi pravicami. V komunikacijskih orodjih se uporabljajo ločeni kanali, ki so dostopni le določenim skupinam zaposlenih. Takšna razdelitev omogoča, da imajo zaposleni dostop le do projektov in vsebin, pri katerih dejansko sodelujejo, druge vsebine pa jim niso vidne.

Dostop do oblačnih storitev je omogočen iz službenih delovnih računalnikov ter iz mobilnih naprav zaposlenih, na katerih so nameščene ustrezne aplikacije. Dostop iz zasebnih računalnikov ni dovoljen. Takšna omejitev zmanjšuje število potencialnih dostopnih točk in omogoča boljši nadzor nad uporabo oblačnih sistemov.

Nadzor nad dostopi in uporabo oblačnih storitev izvaja informacijska podpora predvsem ob zaznanih težavah ali nepravilnostih. Evidenca dostopov in aktivnosti se hrani na lokalnih sistemih podjetja, kar omogoča dodatno sledljivost in pregled nad uporabo oblačnih orodij. Upravljanje dostopa v oblačnih sistemih je tako tesno povezano z notranjo organizacijo dela in vlogo informacijske podpore.

6.4 Omejitve in tveganja oblačnega shranjevanja podatkov

Kljub temu da se oblačno shranjevanje v podjetju uporablja v omejenem in nadzorovanem obsegu, je pri takšnem pristopu treba upoštevati določene omejitve in tveganja. Ta izhajajo predvsem iz dejstva, da oblačne storitve temeljijo na infrastrukturi zunanjih ponudnikov, nad katero podjetje nima neposrednega tehničnega nadzora.

Ena izmed pomembnejših omejitev oblačnega shranjevanja je zmanjšan nadzor nad podatkovnim okoljem. Upravljanje infrastrukture, razpoložljivost storitev in notranji varnostni mehanizmi so v domeni ponudnika oblačnih storitev. Čeprav podjetje v oblak ne shranjuje raziskovalnih ali eksperimentalnih podatkov, takšna odvisnost predstavlja omejitev v primerjavi z lokalnim shranjevanjem, kjer ima podjetje popoln nadzor nad sistemi in podatki.

Tveganje predstavlja tudi uporaba skupnih uporabniških računov pri določenih oblačnih orodjih. Takšna ureditev poenostavi organizacijo dostopa, vendar lahko zmanjša natančno sledljivost posameznih aktivnosti uporabnikov. V primeru napak ali neustrezne uporabe je zato težje določiti odgovornost posameznika, kar predstavlja omejitev z vidika notranjega nadzora.

Oblačno shranjevanje je neposredno odvisno tudi od delovanja internetne povezave. V primeru motenj ali nedosegljivosti oblačnih storitev je dostop do vsebin omejen, kar lahko vpliva na potek dela, predvsem pri komunikaciji in organizaciji aktivnosti. Čeprav takšne situacije ne vplivajo na raziskovalne podatke, lahko začasno otežijo koordinacijo dela med zaposlenimi.

Dodatno tveganje predstavlja človeški dejavnik. Kljub obstoječim neformalnim dogovorom o tem, katere vrste podatkov se ne shranjujejo v oblak, obstaja možnost napačne presoje uporabnika. Učinkovitost omejevanja tveganj je zato v veliki meri odvisna od ozaveščenosti zaposlenih in njihovega razumevanja razlik med lokalnim in oblačnim shranjevanjem podatkov.

Zaradi navedenih omejitev in tveganj podjetje oblačno shranjevanje uporablja premišljeno in omejeno na podporne vsebine. Takšna ureditev omogoča uporabo prednosti oblaka brez vključevanja podatkov, ki bi zahtevali strožji varnostni nadzor.

7. PRIMERJAVA LOKALNEGA IN OBLAČNEGA SISTEMA V PODJETJU

7.1 Primerjava varnosti

Varnost shranjevanja podatkov v podjetju je zagotovljena z različnimi pristopi, odvisno od tega, ali gre za lokalno ali oblačno okolje. Obe rešitvi imata jasno opredeljeno vlogo, pri čemer so varnostni ukrepi prilagojeni vrsti podatkov, ki se hranijo v posameznem okolju. Razlike med lokalnim in oblačnim shranjevanjem se kažejo predvsem v stopnji nadzora, načinu upravljanja dostopov ter vlogi posameznega okolja v delovnih procesih podjetja.

Pri lokalnem shranjevanju podatkov je varnost zasnovana celostno in temelji na neposrednem nadzoru nad infrastrukturo. Podjetje ima popoln nadzor nad fizično lokacijo strežnikov, omrežno segmentacijo, dodeljevanjem dostopov ter postopki varnostnega kopiranja. Lokalni sistemi predstavljajo primarno okolje za shranjevanje raziskovalnih, laboratorijskih in drugih ključnih podatkov. Varnostni ukrepi so neposredno povezani z vlogo informacijske podpore, ki upravlja dostop, nadzira delovanje sistemov in zagotavlja odzivnost v primeru tehničnih težav.

V oblačnem okolju je varnost zasnovana drugače, saj temelji na kombinaciji notranjih omejitev in varnostnih mehanizmov ponudnika oblačnih storitev. Podjetje nima neposrednega vpliva na infrastrukturo oblaka, zato se varnost zagotavlja predvsem z nadzorom dostopov, uporabo dodatnih preverjanj pri prijavi ter z omejevanjem vrst podatkov, ki se shranjujejo v oblak. V oblačno okolje se shranjujejo zgolj podatki srednje občutljivosti, kar zmanjšuje tveganje v primeru morebitnih varnostnih incidentov.

Pomembna razlika med lokalnim in oblačnim shranjevanjem je stopnja nadzora nad podatkovnim okoljem. Lokalni sistemi omogočajo neposreden tehnični in organizacijski nadzor, medtem ko je pri oblačnih storitvah del odgovornosti prenesen na zunanjega ponudnika. To vpliva tudi na način obravnave varnosti, saj podjetje lokalno okolje obravnava kot varnejše in primernejše za shranjevanje kritičnih podatkov, oblačno okolje pa kot dopolnilo za podporne dejavnosti.

Razlike med obema pristopoma se kažejo tudi v vsakodnevni praksi. Pri iskanju starejših eksperimentov se je v določenih primerih izkazalo, da je uporaba oblačnih komunikacijskih orodij, ki omogočajo iskanje po ključnih besedah, hitrejša in preglednejša, zlasti ob večjem številu izvedenih eksperimentov. Ob več letih dela in več sto eksperimentih letno postane

sledljivost zgodovine raziskovalnega dela zahtevnejša, zato oblačna orodja v praksi dopolnjujejo lokalno shranjevanje podatkov. Kljub temu se zaposleni zavedajo razlike med obema okoljema, saj lokalni sistemi ostajajo primarno mesto za shranjevanje podatkov zaradi višje stopnje varnosti, oblačno okolje pa se uporablja predvsem zaradi večje uporabnosti in preglednosti pri organizaciji dela.

Razlika se kaže tudi v načinu upravljanja dostopov. Pri lokalnem shranjevanju so dostopi strogo vezani na notranjo infrastrukturo podjetja, informacijska podpora pa ima neposreden nadzor nad uporabniškimi pravicami in delovanjem sistemov. Pri oblačnih storitvah je dostop omogočen tudi preko mobilnih naprav, vendar z dodatnimi omejitvami in nadzorom, kar omogoča večjo prilagodljivost pri delu, hkrati pa zahteva večjo pozornost pri upravljanju uporabniških pravic.

Podjetje varnost lokalnega in oblačnega shranjevanja obravnava različno glede na vlogo posameznega okolja. Lokalno shranjevanje je namenjeno zaščiti podatkov in temelji na neposrednem nadzoru nad infrastrukturo, medtem ko ima oblačno shranjevanje podporno vlogo, usmerjeno predvsem v komunikacijo in organizacijo dela.

7.2 Primerjava dostopnosti in hitrosti dela

Dostopnost in hitrost dela se pri lokalnem in oblačnem shranjevanju podatkov razlikujeta glede na namen uporabe posameznega okolja. Obe rešitvi imata v podjetju jasno določeno vlogo, kar se odraža tudi v načinu vsakodnevnega dela zaposlenih.

Lokalni strežniški sistemi so dostopni izključno znotraj omrežja podjetja. Dostop do lokalnih podatkov od doma ni omogočen, razen v izjemnih primerih, kar pomeni, da je delo z lokalnimi sistemi vezano na fizično prisotnost v podjetju. Takšna omejitev vpliva na dostopnost, vendar hkrati povečuje nadzor nad podatki in zmanjšuje izpostavljenost zunanjim tveganjem.

Hitrost dela z lokalnimi podatki je znotraj omrežja podjetja zelo dobra in stabilna. Po zaključku eksperimenta se poročila in rezultati takoj shranijo na lokalni strežnik, kjer so na voljo vsem pooblaščenim uporabnikom. Delo z večjimi datotekami, kot so analize in slikovno gradivo, je lokalno hitrejše kot v oblačnem okolju, saj ni odvisno od internetne povezave.

Oblačno okolje je dostopno kadarkoli, če je na voljo internetna povezava. Dostop do oblačnih storitev ne zahteva posredovanja informacijske podpore, kar omogoča večjo fleksibilnost pri uporabi. Oblak se v praksi izkaže kot zelo učinkovit pri komunikaciji, iskanju informacij,

pregledovanju zapiskov in spremljanju poteka dela. Iskanje po ključnih besedah in pregled zgodovine pogovorov omogočata hiter dostop do informacij, ki so pomembne za razumevanje poteka projektov.

Pri oblačnem shranjevanju je hitrost dela neposredno odvisna od delovanja internetne povezave. Brez dostopa do interneta oblačne storitve niso dosegljive, medtem ko lokalni sistemi v takšnih primerih še vedno delujejo. V praksi se oblak uporablja predvsem za hiter pregled informacij in usklajevanje, ne pa za obdelavo večjih ali občutljivejših podatkov.

Zaposleni se pri delu zavestno odločajo, katero okolje uporabiti glede na vrsto naloge. Poročila, rezultati in drugi končni izhodi eksperimentov se shranjujejo izključno na lokalne sisteme, medtem ko se ideje, razprave, komunikacija in organizacijski zapisi pogosto vodijo v oblačnem okolju. Takšna delitev omogoča učinkovito delo, pri katerem se prednosti obeh pristopov dopolnjujejo.

Razlike v dostopnosti in hitrosti dela med lokalnim in oblačnim shranjevanjem so povzete v tabeli 7.2.

Tabela 7.2: Primerjava dostopnosti in hitrosti dela pri lokalnem in oblačnem shranjevanju podatkov

Vidik	Lokalno shranjevanje	Oblačno shranjevanje
Dostopnost	Dostopno samo znotraj podjetja	Dostopno kjerkoli z internetno povezavo
Dostop od doma	Ni omogočen	Omogočen preko spleta ali aplikacij
Odvisnost od interneta	Neodvisno od interneta	Popolnoma odvisno od interneta
Hitrost pri delu z večjimi datotekami	Visoka in stabilna	Omejena z internetno povezavo
Hitrost iskanja informacij	Odvisna od strukture map	Hitro iskanje po tabelah eksperimentov
Tipične naloge	Poročila, analize, rezultati	Komunikacija, zapiski, organizacija

Vir: Lastna priprava

7.3 Primerjava stroškov

Stroškovni vidik predstavlja pomemben dejavnik pri primerjavi lokalnega in oblačnega shranjevanja podatkov, saj obe rešitvi temeljita na različnih finančnih modelih. Razlike se kažejo predvsem v strukturi stroškov, časovni porazdelitvi izdatkov ter v načinu upravljanja infrastrukture.

Lokalno shranjevanje podatkov zahteva začetno investicijo v strojno opremo ter stalno vzdrževanje sistema. Podjetje uporablja lastno strežniško infrastrukturo, kar pomeni, da je potrebno redno posodabljanje, nadgrajevanje in občasna zamenjava strojne opreme. Te aktivnosti izvaja notranja informacijska podpora, ki skrbi za nemoteno delovanje sistemov. Stroški lokalne infrastrukture se zato pojavljajo periodično, praviloma vsako leto, ko se sistem prilagaja rastočim potrebam podjetja ali tehnološkemu razvoju.

Za oblačne storitve podjetje uporablja naročniški model. Stroški so vezani na mesečne naročnine, pri čemer oblačne storitve uporablja več zaposlenih preko skupnih uporabniških računov z različnih naprav. Takšen pristop omogoča bolj predvidljive stroške, saj so izdatki enakomerno razporejeni skozi čas. Hkrati pa se oblačne storitve sčasoma spreminjajo, kar lahko vpliva na funkcionalnosti ali pogoje uporabe, ne pa nujno na samo strukturo stroškov.

Primerjava obeh pristopov pokaže, da lokalna infrastruktura zahteva višje začetne in občasne investicije, vendar omogoča dolgoročno stabilnost in nadzor nad sistemi. Oblačno shranjevanje po drugi strani pomeni nižje začetne stroške, vendar prinaša stalne operativne izdatke v obliki naročnin. V podjetju stroški niso dejavnik pri odločitvi, kateri podatki se hranijo lokalno in kateri v oblaku, temveč ima pri tem glavno vlogo varnostni vidik.

Podjetje lokalno infrastrukturo obravnava predvsem kot dolgoročno investicijo, namenjeno zaščiti ključnih podatkov in podpori raziskovalnega dela. Oblačne storitve pa predstavljajo operativni strošek, ki je upravičen zaradi večje preglednosti, organizacije dela in podpore komunikaciji. Takšna razdelitev omogoča uravnotežen pristop k stroškom, pri katerem se finančni vidik dopolnjuje z varnostnimi in organizacijskimi zahtevami.

7.4 Primerjava nadzora in upravljanja

Pri uporabi lokalnega in oblačnega shranjevanja podatkov se v podjetju jasno razlikujeta način nadzora in upravljanja informacijskega okolja. Lokalni sistemi omogočajo neposreden vpliv na delovanje infrastrukture, dostop do podatkov in upravljanje uporabniških pravic, medtem ko je pri oblačnih storitvah del upravljanja vezan na zunanjega ponudnika. Zaradi tega se vloga informacijske podpore in stopnja nadzora nad sistemi med obema pristopoma bistveno razlikujeta.

Pri lokalnem shranjevanju ima podjetje popoln nadzor nad celotnim informacijskim okoljem. Upravljanje strežnikov, dostopov, uporabniških pravic, varnostnih kopij in delovanja sistemov poteka znotraj podjetja. Informacijska podpora ima neposreden vpogled v stanje infrastrukture in možnost takojšnjega ukrepanja v primeru tehničnih težav ali nepravilnosti. Takšna ureditev omogoča hitro odzivnost, jasne odgovornosti in popoln nadzor nad podatki ter sistemi.

Upravljanje lokalne infrastrukture vključuje tudi redno vzdrževanje in nadgrajevanje strojne ter programske opreme. Odločitve glede sprememb sistema, nadgradenj ali prilagoditev so v celoti

v domeni podjetja, kar omogoča prilagajanje informacijskega okolja specifičnim potrebam raziskovalnega dela. Ta stopnja nadzora je še posebej pomembna pri delu z občutljivimi podatki, kjer so zahteve glede varnosti in sledljivosti visoke.

Pri oblačnem shranjevanju je nadzor nad infrastrukturo delno prenesen na ponudnika storitev. Podjetje nima neposrednega vpliva na tehnično delovanje sistemov, posodobitve ali notranje varnostne mehanizme oblaka. Upravljanje se zato osredotoča predvsem na dodeljevanje uporabniških pravic, nadzor nad dostopi in določanje pravil uporabe oblačnih storitev. Informacijska podpora v tem primeru nastopa predvsem v vlogi administratorja dostopov in nadzornika uporabe, manj pa kot upravljavec same infrastrukture.

Razlika v nadzoru se odraža tudi v vsakodnevnem delu. Pri lokalnem okolju informacijska podpora aktivno spremlja delovanje sistemov in se ob težavah takoj vključi v reševanje. Pri oblačnih storitvah je vloga informacijske podpore bolj omejena, saj se posegi izvajajo predvsem ob zaznanih težavah ali nepravilnostih, medtem ko je del odgovornosti za delovanje sistema na strani ponudnika.

Na podlagi primerjave je razvidno, da lokalno shranjevanje omogoča višjo stopnjo nadzora in neposredno upravljanje celotnega podatkovnega okolja. Oblačno shranjevanje pa zahteva drugačen pristop, pri katerem se podjetje osredotoča na upravljanje dostopov in uporabo storitev, medtem ko je tehnični nadzor nad infrastrukturo omejen. Takšna razdelitev vlog je skladna z namenom uporabe obeh okolij in odraža zavestno odločitev podjetja glede upravljanja podatkov.

7.5 Ključne prednosti in slabosti obeh pristopov

Na podlagi primerjave lokalnega in oblačnega shranjevanja podatkov je mogoče jasno opredeliti prednosti in omejitve obeh pristopov. V podjetju se lokalni in oblačni sistemi ne izključujejo, temveč se uporabljajo dopolnilno, pri čemer ima vsak pristop svojo vlogo glede na vrsto podatkov, zahteve po varnosti ter način dela.

Lokalno shranjevanje podatkov omogoča visoko raven nadzora nad infrastrukturo, dostopi in varnostnimi mehanizmi. Podjetje ima neposreden vpliv na upravljanje sistemov, kar je posebej pomembno pri delu z raziskovalnimi, laboratorijskimi in drugimi občutljivimi podatki. Prednost lokalnega pristopa je tudi stabilnost delovanja in neodvisnost od internetne povezave. Slabosti lokalnega shranjevanja se kažejo predvsem v omejeni dostopnosti, saj delo z lokalnimi

sistemi zahteva prisotnost v podjetju, ter v potrebi po rednem vzdrževanju in nadgrajevanju infrastrukture.

Oblačno shranjevanje podatkov prinaša večjo fleksibilnost pri dostopu in podporo sodelovanju med zaposlenimi. Oblak omogoča hiter pregled informacij, enostavno komunikacijo in boljšo organizacijo dela, zlasti pri idejah, zapiskih in usklajevanju projektov. Slabosti oblačnega pristopa so predvsem omejen nadzor nad infrastrukturo, odvisnost od internetne povezave in večja izpostavljenost zunanjim tveganjem, zaradi česar se v oblak ne shranjujejo ključni raziskovalni podatki.

Pregled ključnih prednosti in slabosti obeh pristopov je povzet v tabeli 7.5.

Tabela 7.5.: Primerjava lokalnega in oblačnega pristopa

Vidik	**Lokalno shranjevanje**	**Oblačno shranjevanje**
Nadzor nad podatki	Popoln nadzor znotraj podjetja	Delni nadzor, odvisen od ponudnika
Varnost	Primernejše za občutljive podatke	Omejena uporaba za manj občutljive podatke
Dostopnost	Omejena na interno omrežje	Dostopno kjerkoli z internetom
Hitrost dela	Visoka in stabilna znotraj omrežja	Odvisna od internetne povezave
Stroški	Investicija in redno vzdrževanje	Stalni naročniški stroški
Podpora sodelovanju	Omejena	Zelo dobra

Vir: Lastna priprava

Na podlagi primerjave je razvidno, da kombinacija lokalnega in oblačnega shranjevanja omogoča uravnotežen pristop k upravljanju podatkov. Lokalni sistemi zagotavljajo varnost in nadzor nad informacijami, oblačne storitve pa dopolnjujejo delovne procese z vidika organizacije, komunikacije in preglednosti.

8. VARNOSTNA ANALIZA IN OCENA TVEGANJ

8.1 Tveganja pri lokalni infrastrukturi

Uporaba lokalne infrastrukture za shranjevanje podatkov poleg številnih prednosti prinaša tudi določena tveganja, ki jih je treba prepoznati in ustrezno obvladovati. Ta tveganja izhajajo tako iz tehničnih omejitev kot tudi z organizacijskih in varnostnih vidikov delovanja sistema.

Ena izmed osnovnih tehničnih tveganj pri lokalni infrastrukturi je možnost okvare strojne opreme. Okvare strežnikov ali podatkovnih nosilcev so kljub sodobni tehnologiji vedno možne. V podjetju se to tveganje zmanjšuje z uporabo več varnostnih kopij, pri čemer je ena izmed njih shranjena na ločeni lokaciji. Takšna ureditev bistveno zmanjša verjetnost izgube podatkov tudi v primeru hujših okvar ali nepredvidenih dogodkov. Kljub temu lokalna infrastruktura ostaja odvisna od delovanja električnega omrežja, hlajenja in fizičnih pogojev prostora, v katerem so strežniki nameščeni.

Organizacijska tveganja so povezana predvsem z upravljanjem sistema in razpoložljivostjo znanja. Delovanje lokalne infrastrukture je v veliki meri odvisno od informacijske podpore, saj je tehnično znanje skoncentrirano na omejeno število oseb. To pomeni, da lahko v primeru odsotnosti ali preobremenjenosti IT-podpore pride do zamikov pri reševanju težav ali pri dodeljevanju dostopov. Obstaja tudi tveganje človeških napak pri upravljanju sistema, zlasti pri nastavljanju uporabniških pravic, čeprav se to tveganje zmanjšuje z internimi preverjanji ob dodeljevanju dostopov.

Dostopnost podatkov predstavlja dodatno tveganje, predvsem za zaposlene, ki niso del informacijske podpore. Lokalni sistemi zahtevajo prisotnost v podjetju ali uporabo določenih dostopnih mehanizmov, kar pomeni, da v primeru omejenega fizičnega dostopa ali tehničnih težav zaposleni začasno ne morejo dostopati do vseh potrebnih podatkov. V praksi se to kaže tudi v primerih, ko zaposleni nimajo ustreznih pravic za dostop do določenih vsebin in morajo zaprositi za dodatna dovoljenja, kar lahko upočasni delo.

Varnostna tveganja pri lokalni infrastrukturi so delno povezana z notranjim okoljem. Sistem temelji na zaupanju med zaposlenimi, zato obstaja možnost nenamernih napak ali notranjih zlorab. Ta tveganja se zmanjšujejo z uporabo uporabniških pravic, omejevanjem dostopov ter rednim shranjevanjem varnostnih kopij, ki omogočajo obnovo podatkov v primeru brisanja ali poškodbe.

Na splošno so tveganja, povezana z lokalno infrastrukturo, v podjetju prepoznana in zavestno sprejeta. Njihovo obvladovanje temelji na kombinaciji tehničnih rešitev, organizacijskih pravil in aktivne vloge informacijske podpore. Takšen pristop omogoča stabilno delovanje sistema in hkrati zmanjšuje vpliv morebitnih tveganj na raziskovalno in razvojno delo.

8.2 Tveganja pri oblačnem shranjevanju podatkov

Uporaba oblačnega shranjevanja podatkov v podjetju prinaša določena tveganja, ki so drugačne narave kot pri lokalni infrastrukturi. Ta tveganja so predvsem povezana z organizacijskimi dejavniki, zunanjimi ponudniki storitev ter načinom uporabe oblačnih orodij v vsakodnevnem delu.

Ena izmed glavnih nevarnosti oblačnega shranjevanja je možnost, da se v oblak po pomoti shranijo podatki, ki tja ne sodijo. V praksi se je že zgodilo, da so bile v oblačnih orodjih zapisane informacije, ki so vsebovale več podrobnosti o projektih ali eksperimentih, kot bi bilo zaželeno. Nadzor nad vsebino v oblaku je manj strog kot pri lokalnih sistemih, saj temelji predvsem na dogovorih in ozaveščenosti zaposlenih.

Pomembno tveganje predstavlja tudi odvisnost od zunanjega ponudnika oblačnih storitev. Podjetje nima neposrednega nadzora nad fizično lokacijo shranjevanja podatkov, prav tako pa nima vpliva na notranje tehnične in varnostne postopke ponudnika. Obstaja tudi tveganje sprememb pogojev uporabe ali delovanja storitev, kar lahko vpliva na način uporabe oblaka. Ker je delovanje oblačnih storitev v celoti vezano na zunanje okolje, je podjetje v tem pogledu omejeno pri upravljanju sistema.

Tveganja so prisotna tudi na področju dostopov in upravljanja uporabnikov. Nadzor nad uporabniškimi pravicami v oblaku je manj centraliziran kot pri lokalni infrastrukturi, saj je del upravljanja vezan na same oblačne platforme. Čeprav do sedaj ni prišlo do nepooblaščenih dostopov, takšen način upravljanja predstavlja potencialno tveganje, zlasti ob uporabi več naprav in skupnih uporabniških računov.

Oblačno shranjevanje je v celoti odvisno od internetne povezave. V primeru izpada interneta ali težav z omrežjem dostop do oblačnih storitev ni mogoč, kar lahko začasno oteži delo, predvsem pri komunikaciji in organizaciji aktivnosti. Čeprav večjih izpadov oblačnih storitev v praksi ni bilo, ostaja odvisnost od internetne povezave pomemben dejavnik tveganja.

Organizacijsko tveganje predstavlja tudi način dojemanja oblaka med zaposlenimi. Oblak se pogosto uporablja kot bolj neformalno okolje za komunikacijo in izmenjavo idej, kar lahko poveča tveganje nenadzorovanega deljenja informacij. Kljub temu so tveganja, povezana z oblačnim shranjevanjem, v podjetju prepoznana in zavestno upoštevana. Prav zaradi teh tveganj se oblak uporablja omejeno in predvsem za podporne vsebine, medtem ko se ključni podatki hranijo v lokalnem okolju.

8.3 Identifikacija ranljivosti v obstoječem sistemu

Na podlagi analize lokalnega in oblačnega shranjevanja podatkov je mogoče v obstoječem informacijskem sistemu podjetja prepoznati več ranljivosti, ki ne pomenijo nujno neposrednega varnostnega incidenta, vendar lahko v določenih okoliščinah povečajo tveganje za neustrezno ravnanje s podatki. Identifikacija teh ranljivosti je pomembna za razumevanje, kje so potencialne šibke točke sistema.

Z vidika tehnične infrastrukture večjih ranljivosti ni zaznati. Sistemi se redno posodabljajo, dostop do strežnikov je tehnično omejen, prav tako ni zaznanih kritičnih točk brez redundance. Takšna ureditev zmanjšuje možnost tehničnih zlorab ali izpadov zaradi zastarele opreme. Kljub temu lokalna infrastruktura ostaja kompleksna in zahteva stalno strokovno upravljanje, kar pomeni, da je delovanje sistema močno odvisno od informacijske podpore.

Procesne ranljivosti se kažejo predvsem pri upravljanju uporabniških pravic. Čeprav so postopki dodeljevanja dostopov formalno opredeljeni in dokumentirani, se v praksi dogaja, da se pravice po zaključku projektov ne odvzamejo sistematično. Posledično lahko uporabniki ohranijo dostop do podatkov, ki jih za svoje delo ne potrebujejo več. Takšna ranljivost ne pomeni nujno zlorabe, vendar povečuje izpostavljenost sistema notranjim tveganjem.

Pomemben vir ranljivosti predstavlja tudi človeški dejavnik. Zaposleni se načeloma zavedajo razlike med lokalnim in oblačnim okoljem, vendar v praksi lahko pride do napačne presoje glede tega, katere informacije so primerne za deljenje v oblaku. Varnostno ozaveščanje zaposlenih poteka predvsem neformalno, skozi prakso in interne dogovore, kar pomeni, da ni enotnega in sistematičnega pristopa k obravnavi varnostnih vprašanj.

Pri uporabi oblačnih storitev so ranljivosti povezane predvsem z upravljanjem dostopov in preglednostjo uporabe. Čeprav do sedaj ni bilo zaznanih nepooblaščenih dostopov, obstaja tveganje, da ob odhodu zaposlenega dostop do oblačnih storitev ne bi bil pravočasno omejen.

Poleg tega informacijska podpora nima vedno popolnega vpogleda v spremembe načina uporabe oblačnih orodij, kar lahko oteži pravočasno zaznavanje neustreznih praks.

Na splošno so ranljivosti v obstoječem sistemu delno prepoznane, vendar ne vedno sistematično obravnavane. Večina zaznanih ranljivosti je organizacijske in procesne narave, ne tehnične. Njihovo zmanjševanje bi bilo mogoče predvsem z izboljšanjem postopkov upravljanja dostopov, doslednejšim pregledovanjem pravic ter z dodatnimi tehničnimi in organizacijskimi ukrepi, kar predstavlja izhodišče za naslednje poglavje, v katerem so predstavljeni predlogi izboljšav.

8.4 Threat-modeling: najverjetnejši scenariji

Na podlagi analize obstoječega informacijskega sistema je mogoče izpostaviti nekaj najverjetnejših scenarijev varnostnih incidentov, ki ne izhajajo iz tehničnih napak, temveč predvsem iz načina uporabe sistemov in človeškega faktorja.

Pri lokalni infrastrukturi predstavlja najverjetnejši scenarij človeška napaka. Ta se lahko kaže v napačnem shranjevanju podatkov, neustreznem upravljanju dostopov ali v neupoštevanju notranjih postopkov. Čeprav so tehnični sistemi stabilni in zaščiteni, je delovanje lokalnega okolja v veliki meri odvisno od pravilne uporabe s strani zaposlenih in informacijske podpore.

Pri oblačnem shranjevanju podatkov je najverjetnejši scenarij povezan z deljenjem prevelike količine informacij. Oblak se uporablja predvsem za komunikacijo in izmenjavo idej, zato obstaja večja možnost, da se v pogovorih ali zapisih pojavijo podatki, ki bi morali ostati znotraj lokalnega okolja. Takšni primeri praviloma niso namerni, temveč posledica neformalnega načina uporabe oblačnih orodij.

Glede izvora groženj je težko jasno ločiti med notranjimi in zunanjimi viri. Notranji uporabniki lahko nenamerno povzročijo varnostne incidente zaradi nepozornosti ali napačne presoje, medtem ko zunanje grožnje predstavljajo potencialno tveganje predvsem zaradi odvisnosti od internetne povezave in zunanjih ponudnikov storitev. V podjetju se oba vidika obravnavata kot možna, vendar ne kot najpogostejša.

V primeru varnostnega incidenta bi bil najverjetnejši vpliv predvsem na organizacijo dela. Motnje v dostopnosti podatkov ali v komunikacijskih kanalih bi lahko dolgoročno vplivale na potek raziskovalnih in razvojnih aktivnosti, tudi če ne bi prišlo do neposredne izgube podatkov.

Zato je prepoznavanje teh scenarijev pomembno izhodišče za oblikovanje ustreznih preventivnih ukrepov.

8.5 Vpliv kibernetskih incidentov na delovne procese

Kibernetski incidenti v podjetju ne bi imeli le tehničnih posledic, temveč bi se predvsem odrazili na organizaciji in poteku dela. Motnje v dostopnosti lokalnih ali oblačnih sistemov bi lahko začasno upočasnile raziskovalne in administrativne procese ter otežile sodelovanje med zaposlenimi.

Pri lokalni infrastrukturi bi morebitni incidenti, kot so napačna dovoljenja ali omejen dostop do podatkov, povzročili zamike pri delu, saj bi zaposleni morali čakati na posredovanje informacijske podpore. Čeprav so podatki zaščiteni z varnostnimi kopijami, lahko takšne motnje vplivajo na časovno razporeditev nalog in potek projektov.

Pri oblačnih storitvah bi bil vpliv incidentov najbolj opazen pri komunikaciji in usklajevanju dela. Omejen dostop do komunikacijskih orodij ali neustrezna raba teh orodij bi lahko povzročila nejasnosti pri dogovorih, slabšo preglednost nad nalogami ter zmanjšano učinkovitost sodelovanja.

Na dolgi rok lahko ponavljajoči se manjši incidenti vplivajo na zaupanje zaposlenih v informacijski sistem in povečajo potrebo po dodatnih preverjanjih ter usklajevanjih. Zato je razumevanje vpliva kibernetskih incidentov na delovne procese pomembno za načrtovanje izboljšav in preventivnih ukrepov, ki so obravnavani v naslednjem poglavju.

9. PREDLOGI IZBOLJŠAV

9.1 Predlagane varnostne nadgradnje

Na podlagi analize tveganj in identificiranih ranljivosti v obstoječem sistemu je mogoče predlagati več varnostnih nadgradenj, ki ne zahtevajo večjih sprememb infrastrukture, temveč temeljijo predvsem na izboljšanju organizacijskih in upravljavskih postopkov.

Ena izmed predlaganih nadgradenj je rednejši pregled uporabniških pravic. Glede na število zaposlenih in projektno naravo dela bi bil smiseln pogostejši pregled dostopov, na primer mesečno, kar bi zmanjšalo tveganje, da uporabniki ohranijo dostop do podatkov, ki jih za svoje delo ne potrebujejo več. Takšen pristop bi izboljšal preglednost in nadzor nad uporabo lokalnega sistema.

Dodatna varnostna nadgradnja se nanaša na jasnejšo formalizacijo postopkov, povezanih z dodeljevanjem in odvzemanjem dostopov. Čeprav v podjetju že obstajajo pisna pravila, bi bila koristna njihova nadgradnja v obliki kratkih in enostavnih internih navodil za zaposlene. Ta bi lahko zmanjšala tveganje napačne uporabe sistema in izboljšala doslednost pri ravnanju s podatki.

Upravljanje dostopov trenutno poteka ročno, kar predstavlja organizacijsko ranljivost. Postopno uvajanje enostavnih izboljšav, kot so bolj sistematični pregledi pravic ali delna avtomatizacija določenih korakov, bi lahko povečalo raven varnosti in hkrati razbremenilo informacijsko podporo.

Predlagane varnostne nadgradnje so izvedljive postopoma in brez večjih tehničnih posegov. Njihov namen je povečati varnost in preglednost obstoječega sistema ter zmanjšati vpliv organizacijskih in človeških dejavnikov na varnost podatkov.

9.2 Optimizacija obstoječega načina dela

Poleg varnostnih nadgradenj je mogoče obstoječi način dela dodatno optimizirati z organizacijskimi ukrepi, ki izboljšujejo preglednost, zmanjšujejo možnost napak in olajšajo vsakodnevno delo zaposlenih. Takšne optimizacije ne zahtevajo uvajanja novih sistemov, temveč temeljijo na bolj enotni in dosledni uporabi že obstoječih rešitev.

Ena izmed možnosti je jasnejša opredelitev, katere vrste vsebin sodijo v lokalno okolje in katere v oblačne storitve. Čeprav se zaposleni te razlike načeloma zavedajo, bi kratek interni dokument

z osnovnimi usmeritvami pripomogel k večji doslednosti pri shranjevanju podatkov in komunikaciji. Takšen dokument bi lahko služil kot praktično vodilo, zlasti za nove zaposlene.

Optimizacija se lahko nanaša tudi na organizacijo podatkov v lokalnem sistemu. Zaradi projektne narave dela in stalnega nastajanja novih vsebin bi bila občasna reorganizacija map smiselna, saj bi izboljšala preglednost in olajšala iskanje starejših podatkov. Redno prilagajanje strukture map dejanskim potrebam projektov bi zmanjšalo tveganje nepreglednosti in podvajanja vsebin.

Pomemben vidik optimizacije predstavlja tudi ozaveščanje zaposlenih. Letni kratki pregledi ali opozorila s strani informacijske podpore glede varne in ustrezne rabe lokalnih ter oblačnih sistemov bi lahko prispevali k večji odgovornosti uporabnikov in zmanjšanju nenamernih napak. Takšen pristop podpira kulturo varnega ravnanja s podatki brez dodatnih administrativnih obremenitev.

Cilj predlaganih optimizacij je ohraniti obstoječo kombinacijo lokalnega in oblačnega shranjevanja, hkrati pa izboljšati preglednost in zmanjšati možnost napak v vsakodnevnih delovnih procesih. S tem se krepita učinkovitost dela in dolgoročna zanesljivost informacijskega okolja podjetja.

9.3 Izboljšave varnostnih kopij in dostopnih pravic

Obstoječa ureditev varnostnih kopij in upravljanja dostopnih pravic v podjetju je vzpostavljena premišljeno in zagotavlja visoko stopnjo zaščite podatkov. Varnostne kopije se izvajajo avtomatsko večkrat dnevno, po potrebi pa tudi ročno, kar omogoča hitro odzivanje v primeru tehničnih težav ali nenamernih sprememb podatkov. Poleg tega se redno preverja uspešnost varnostnih kopij, kar zmanjšuje tveganje, da bi bile te neuporabne v primeru dejanske potrebe po obnovi sistema.

Kljub ustrezni vzpostavitvi sistema obstaja možnost manjših izboljšav, predvsem na ravni preglednosti in dolgoročne zanesljivosti. Ena izmed takšnih izboljšav je ohranjanje jasne dokumentacije o delovanju varnostnih kopij, odgovornostih informacijske podpore in postopkih obnove podatkov. Čeprav so ti postopki že urejeni, bi njihova sistematična dokumentacija dodatno zmanjšala odvisnost od posameznikov in olajšala ukrepanje v nepredvidenih situacijah.

Upravljanje dostopnih pravic je v podjetju centralizirano in se redno prilagaja spremembam vlog zaposlenih. Ob vsaki spremembi delovnih nalog se preveri ustreznost obstoječih dovoljenj, kar zmanjšuje tveganje nepooblaščenega dostopa. Možna izboljšava na tem področju je bolj jasno razlikovanje med kritičnimi in manj kritičnimi podatki, pri čemer bi bil dostop do manj občutljivih vsebin omogočen hitreje, medtem ko bi za ključne podatke ostali strožji postopki odobritve.

Predlagane izboljšave ne zahtevajo večjih sprememb obstoječe infrastrukture, temveč temeljijo na nadgradnji obstoječih postopkov. Njihov cilj je povečati preglednost delovanja sistema in hkrati ohraniti visoko raven varnosti, ki je za podjetje zaradi raziskovalne narave dela še posebej pomembna.

9.4 Ocena izvedljivosti in priporočila

Na podlagi izvedene analize je mogoče ugotoviti, da so predlagane varnostne nadgradnje in organizacijske izboljšave v podjetju v veliki meri izvedljive znotraj obstoječega informacijskega okolja. Predlagani ukrepi ne zahtevajo večjih infrastrukturnih sprememb ali uvajanja novih sistemov, temveč temeljijo predvsem na nadgradnji že vzpostavljenih postopkov in bolj dosledni uporabi obstoječih rešitev.

Z vidika izvedljivosti je pomembno, da podjetje že razpolaga z ustrezno tehnično infrastrukturo, jasno razdeljenimi vlogami informacijske podpore ter vzpostavljenimi postopki varnostnega kopiranja in upravljanja dostopnih pravic. Zaradi tega bi bila večina predlaganih izboljšav povezana predvsem z organizacijskimi prilagoditvami, rednim pregledom obstoječih praks ter dodatnim ozaveščanjem zaposlenih, ne pa z večjimi finančnimi vložki.

Priporočljivo je, da podjetje v prihodnje ohrani obstoječo razmejitev med lokalnim in oblačnim shranjevanjem podatkov, saj se je ta v praksi izkazala kot ustrezna glede na naravo raziskovalnega dela. Dodatno pozornost bi bilo smiselno nameniti rednemu pregledu dostopnih pravic, dokumentiranju ključnih varnostnih postopkov ter periodični reorganizaciji podatkovnih struktur, ki sledijo dejanskemu poteku projektov.

Uvedba predlaganih izboljšav bi dolgoročno prispevala k večji preglednosti dela, zmanjšanju možnosti človeških napak in večji odpornosti sistema na morebitne varnostne incidente. Ob upoštevanju obstoječe organizacije in kulture dela so ti ukrepi realni, sorazmerni in v skladu z razvojnimi usmeritvami podjetja.

10. RAZPRAVA

10.1 Interpretacija rezultatov

Rezultati analize lokalnega in oblačnega shranjevanja podatkov kažejo, da izbrani način upravljanja informacij v podjetju temelji na premišljeni razmejitvi med varnostjo in učinkovitostjo dela. Ugotovitve potrjujejo, da lokalna infrastruktura predstavlja osrednji element za shranjevanje raziskovalnih in drugih občutljivih podatkov, medtem ko oblačne storitve opravljajo podporno vlogo pri organizaciji dela in komunikaciji.

Analiza je pokazala, da je uporaba lokalnega shranjevanja utemeljena predvsem z vidika nadzora nad podatki, varnosti in skladnosti z notranjimi zahtevami podjetja. Identificirana tveganja in ranljivosti pri lokalni infrastrukturi niso tehnične narave, temveč so večinoma povezane z organizacijskimi postopki in človeškim faktorjem. To nakazuje, da je osnovna tehnična zasnova sistema ustrezna, izboljšave pa so potrebne predvsem na ravni upravljanja in doslednosti uporabe.

Pri oblačnih storitvah rezultati potrjujejo, da te pomembno prispevajo k boljši preglednosti dela in lažji komunikaciji med zaposlenimi. Hkrati pa analiza tveganj kaže, da oblak zaradi manj strogega nadzora ni primeren za shranjevanje ključnih raziskovalnih podatkov. Takšna omejena uporaba oblaka je zato smiselna in skladna z varnostnimi cilji podjetja.

Primerjalna analiza obeh pristopov kaže, da trenutna kombinacija lokalnega in oblačnega shranjevanja omogoča uravnotežen način dela. Sistem ni zasnovan kot popolnoma zaprt ali popolnoma odprt, temveč kot prilagojeno okolje, ki upošteva naravo raziskovalnega dela in pomen varovanja podatkov. Predlagane izboljšave izhajajo neposredno iz ugotovitev analize in potrjujejo, da večina izzivov ni povezana s pomanjkanjem tehnologije, temveč z organizacijo dela in upravljanjem obstoječih rešitev.

10.2 Omejitve raziskave

Pri interpretaciji rezultatov je treba upoštevati tudi omejitve izvedene raziskave. Analiza temelji na študiji enega podjetja in njegovem konkretnem informacijskem okolju, zato ugotovitev ni mogoče neposredno posplošiti na vsa biotehnološka ali raziskovalna podjetja. Organizacija dela, obseg podatkov in varnostne zahteve se lahko med podjetji bistveno razlikujejo.

Raziskava se je osredotočala predvsem na kvalitativno analizo obstoječih praks, postopkov in organizacijskih rešitev. Kvantitativni podatki, kot so natančni stroški, statistika incidentov ali meritve učinkovitosti, niso bili vključeni, saj za namen naloge niso bili dostopni ali relevantni. Posledično so rezultati utemeljeni predvsem na analizi procesov in strokovni presoji.

Dodatna omejitev raziskave je povezana z varnostnimi razlogi. Zaradi občutljivosti podatkov niso bili podrobno predstavljeni tehnični parametri infrastrukture, natančne varnostne nastavitve ali konkretne arhitekturne rešitve. To omejuje globino tehničnega opisa, vendar ne vpliva na splošne ugotovitve glede upravljanja podatkov in varnostnih pristopov.

Kljub navedenim omejitvam raziskava ponuja realen vpogled v prakso upravljanja podatkov v raziskovalnem okolju ter omogoča oblikovanje utemeljenih zaključkov in priporočil v okviru zastavljenih ciljev diplomske naloge.

10.3 Možnosti nadaljnjega raziskovanja

Na podlagi izvedene analize se odpirajo možnosti za nadaljnje raziskovanje na področju upravljanja in varnosti podatkov v raziskovalnih okoljih. Ena izmed smeri nadaljnjega raziskovanja bi bila primerjalna analiza podobnih informacijskih sistemov v več podjetjih, kar bi omogočilo širši vpogled v različne pristope k lokalnemu in oblačnemu shranjevanju podatkov.

Nadaljnje raziskave bi se lahko osredotočile tudi na bolj poglobljeno analizo učinkovitosti posameznih varnostnih ukrepov, zlasti na področju upravljanja dostopnih pravic in varnostnih kopij. Vključitev kvantitativnih podatkov, kot so časovni prihranki, pogostost napak ali vpliv izboljšav na potek dela, bi omogočila natančnejšo oceno učinkovitosti predlaganih rešitev.

Dodatna možnost nadaljnjega raziskovanja je proučevanje vpliva ozaveščanja zaposlenih na varno ravnanje s podatki. Analiza različnih pristopov k izobraževanju in notranji komunikaciji bi lahko prispevala k boljšemu razumevanju vloge človeškega faktorja pri zagotavljanju informacijske varnosti.

Takšne nadaljnje raziskave bi dopolnile ugotovitve te diplomske naloge in omogočile še celovitejši pogled na upravljanje podatkov v biotehnoloških raziskovalnih okoljih.

11. SKLEP

Namen diplomskega dela je bil predstaviti in analizirati varnostne vidike lokalnega in oblačnega shranjevanja podatkov v biotehnološkem raziskovalnem okolju ter oceniti, kateri pristop ustrezneje podpira varnostne potrebe podjetja. Zaradi narave dela, pri katerem nastajajo občutljivi raziskovalni, eksperimentalni in operativni podatki, je vprašanje ustreznega načina shranjevanja ključno za zagotavljanje zanesljivosti, zaščite informacij in neprekinjenega poteka raziskovalnega procesa.

Zastavljeni cilji diplomskega dela so bili doseženi. V okviru raziskave so bile najprej opredeljene vrste podatkov, ki nastajajo v podjetju, ter njihova razporeditev med lokalno in oblačno infrastrukturo. Analiza je pokazala, da se na lokalnih strežnikih shranjujejo predvsem raziskovalni rezultati, eksperimentalni zapisi, analitična poročila, mikroskopske slike, dokumentacija kakovosti in drugi podatki, ki imajo neposredno znanstveno in poslovno vrednost. Oblačne storitve se uporabljajo predvsem za komunikacijo, organizacijo dela, projektno usklajevanje in podporne vsebine, pri čemer se ključni raziskovalni podatki praviloma ne shranjujejo v oblak.

S tem je bilo odgovorjeno na prvo raziskovalno vprašanje glede razporeditve podatkov med lokalnimi strežniki in oblačnimi storitvami. Ugotovljeno je bilo, da podjetje zavestno ločuje kritične raziskovalne podatke od podpornih informacijskih vsebin, kar zmanjšuje izpostavljenost občutljivih podatkov zunanjim tveganjem.

Drugo raziskovalno vprašanje se je nanašalo na dejavnike, ki vplivajo na odločitev med lokalnim in oblačnim shranjevanjem. Analiza je pokazala, da podjetje pri tej odločitvi upošteva predvsem stopnjo občutljivosti podatkov, zahteve glede sledljivosti, regulativne obveznosti, potrebo po nadzoru dostopa ter stabilnost in zmogljivost sistema. Lokalna infrastruktura se uporablja tam, kjer je potreben višji nadzor nad podatkovnim življenjskim ciklom, medtem ko oblačne storitve podpirajo fleksibilnost, mobilnost in lažje sodelovanje med zaposlenimi.

Tretje raziskovalno vprašanje je obravnavalo varnostne postopke za zaščito podatkov v podjetju. Ugotovljeno je bilo, da sistem vključuje večstopenjsko varnostno kopiranje, omejevanje dostopa preko uporabniških pravic, segmentacijo omrežja ter redno posodabljanje programske opreme. Varnostni mehanizmi so tehnično ustrezni in zagotavljajo zaščito pred izgubo podatkov, nepooblaščenim dostopom ali nenamernimi spremembami. Poseben pomen ima tudi sledljivost dostopov in dosledna organizacija podatkovnih struktur.

Analiza glavnih tveganj pri uporabi lokalnih in oblačnih rešitev je pokazala, da so tveganja različne narave. Pri lokalni infrastrukturi so ključni izzivi povezani z vzdrževanjem strojne opreme, organizacijo dostopov in odvisnostjo od interne IT-podpore. Pri oblačnih rešitvah pa so tveganja vezana predvsem na odvisnost od internetne povezave, lokacijo shranjevanja podatkov in omejen nadzor nad fizično infrastrukturo. Kljub temu analiza ni pokazala kritičnih varnostnih pomanjkljivosti, temveč predvsem organizacijske priložnosti za izboljšave.

Na vprašanje, kako podjetje zagotavlja zaščito podatkov pred izgubo, nepooblaščenim dostopom ali spremembami, je bilo ugotovljeno, da kombinacija tehničnih rešitev in organizacijskih postopkov predstavlja ustrezno raven zaščite. Vendar pa je raziskava pokazala, da večina potencialnih tveganj ne izhaja iz tehnologije same, temveč iz človeškega faktorja in doslednosti pri izvajanju notranjih pravil.

Zadnje raziskovalno vprašanje se je nanašalo na možnosti izboljšav obstoječega sistema. Na podlagi analize so bili predlagani ukrepi, kot so redni pregledi dostopnih pravic, jasnejša interna pravila glede uporabe oblačnih storitev, doslednejša kategorizacija podatkov ter dodatna ozaveščenost zaposlenih glede varnostnih tveganj. Predlagane izboljšave ne zahtevajo večjih infrastrukturnih sprememb, temveč predvsem organizacijsko nadgradnjo obstoječega sistema.

Diplomsko delo potrjuje, da v biotehnološkem raziskovalnem okolju ni mogoče enoznačno opredeliti lokalnega ali oblačnega shranjevanja kot univerzalno boljšega pristopa. Ustreznost je odvisna od vrste podatkov, regulativnih zahtev, organizacije dela in stopnje občutljivosti informacij. Kombiniran pristop, ki jasno ločuje kritične raziskovalne podatke od podpornih vsebin, se je v obravnavanem podjetju izkazal kot učinkovit in sorazmeren naravi dela.

V širšem kontekstu naloga poudarja, da informacijska varnost v raziskovalnih organizacijah ni zgolj tehnični izziv, temveč celovit proces upravljanja, ki vključuje tehnologijo, organizacijo dela in odgovorno ravnanje zaposlenih. Le z usklajenim delovanjem teh elementov je mogoče zagotoviti dolgoročno zaščito podatkov, stabilnost raziskovalnih procesov in varovanje intelektualne lastnine.

Ugotovitve diplomskega dela lahko služijo kot podlaga za nadaljnje izboljšave upravljanja podatkov v podobnih raziskovalnih in razvojnih organizacijah, kjer je varnost informacij neposredno povezana z znanstveno kredibilnostjo, konkurenčnostjo in trajnostnim razvojem podjetja.

12. LITERATURE IN VIRI

ALCOA+ Data Integrity. (2025). *Laboratory Data Integrity Guide*. Pridobljeno iz METTLER TOLEDO: https://www.mt.com/us/en/home/library/guides/laboratory-division/lab-data-integrity/lab-data-integrity-materials.html

Backblaze. (2023). *What's the difference between NAS and SAN?* Pridobljeno iz Backblaze: https://www.backblaze.com/blog/whats-the-diff-nas-vs-san/

Boško, M. (2025). *Network Segmentation: Definition, Benefits, Best Practices*. Pridobljeno iz phoenixNAP: https://phoenixnap.com/blog/network-segmentation

Brelih, A. (2019). Varnost računalništva v oblaku . *Varnost računalništva v oblaku*.

Carbide. (n.d). *Cloud storage vs. local storage: 19 pros and cons*. Pridobljeno iz Carbide: https://carbidesecure.com/resources/cloud-storage-vs-local-storage-19-pros-and-cons/

Chin, K. (5. January 2026). *Top 8 Network Segmentation Best Practices in 2026*. Pridobljeno iz UpGuard: https://www.upguard.com/blog/network-segmentation-best-practices

Cloudfresh. (2024). *Cloudfresh*. Pridobljeno iz On-premises or in the cloud: Overview of the pros and cons: https://cloudfresh.com/en/blog/on-premise-vs-cloud/

Council of Europe. (2012). *Human Rights and Biomedicine*. Pridobljeno iz Guide for Research Ethics Committee Members: https://www.coe.int/en/web/human-rights-and-biomedicine/guide-for-research-ethics-committees-members

Enterprise Networking Planet. (2023). *Enterprise Networking Planet*. Pridobljeno iz 9 Network Segmentation Best Practices to Improve Security: https://www.enterprisenetworkingplanet.com/security/network-segmentation-best-practices/

Evropska unija. (2016). *UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA*. Pridobljeno iz Uradni list Evropske unije: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016R0679

Garbe, D. (12. 9 2025). *On-premises explained: advantages, disadvantages and alternatives* . Pridobljeno iz Softtailor: https://www.softtailor.de/en/blog/on-premises

Google Cloud. (n.d.). *https://cloud.google.com/learn/paas-vs-iaas-vs-saas?utm_source=chatgpt.com*. Pridobljeno iz Google Cloud:

https://cloud.google.com/learn/paas-vs-iaas-vs-saas?utm_source=chatgpt.com#paas-vs-iaas-vs-saas-vs-caas-how-are-they-different

Ial, S. (14. October 2024). *Challenges of On-Premise Local Servers*. Pridobljeno iz Technaureus: https://www.technaureus.com/blog-detail/challenges-of-on-premise-local-servers

IBM. (n.d.). *IaaS, PaaS, SaaS: What's the difference?*. Pridobljeno iz IBM: https://www.ibm.com/think/topics/iaas-paas-saas

Ihonvbere, D. (3. November 2024). *PDCA Cycle of ISO 27001: A Comprehensive Guide*. Pridobljeno iz Tech Prognosis: https://blog.techprognosis.com/pdca-cycle-of-iso-27001-a-comprehensive-guide/

Imperva. (2025). *Data Asset Managment*. Pridobljeno iz Thales cyber security imperva : https://www.imperva.com/learn/data-security/data-asset-management/

INTROSERV. (n.d.). *Varnostno kopiranje podatkov med strežniki* . Pridobljeno iz INTROSERV: https://introserv.com/sl/tutorials/backup-data-between-servers/

Investopedia . (2017). *Understanding Cloud Computing: Benefits, Services, and Security*. Pridobljeno iz Investopedia: https://www.investopedia.com/terms/c/cloud-computing.asp

Ivarnost.si. (brez datuma). *Segmentacija omrežja z vidika kibernetske varnosti*. Pridobljeno iz Ivarnost.si: https://ivarnost.si/segmentacija-omrezja-z-vidika-kibernetske-varnosti/

J. Donelly. (2023). *NAS vs. RAID Storage Differences*. Pridobljeno iz Massive.io: https://massive.io/file-transfer/nas-vs-raid/

Jelenc, D. (2023). Varnost in računalništvo v oblaku: premik k uporabnikom.

Jungco, K. (25. February 2025). *Cloud Storage vs. Local Storage*. Pridobljeno iz TechnologyAdvice: https://technologyadvice.com/blog/information-technology/cloud-storage-vs-local-storage/

Michael E. Whitman, H. J. (2014). *Principles of Information Security.*

Microsoft. (2026). *What is Cybersecurity?* Pridobljeno iz Microsoft: https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity

National Institute of Standards and Technology. (16. April 2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Pridobljeno iz National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Neng W., T. H. (2025). Comparative Study of Data Security: Cloud Storage and Local Storage in.

OECD. (2021). *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring.* OECD.

OECD. (n.d.). *Good Laboratory Practice and Compliance Monitoring*. Pridobljeno iz OECD: https://www.oecd.org/en/topics/sub-issues/testing-of-chemicals/good-laboratory-practice-and-compliance-monitoring.html

P. Diamond. (2020). *Cloud storage vs. on-premises servers: 9 things to keep in mind.* Pridobljeno iz Microsoft: https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

Pandora FMS team |. (2021). *What is RAID? What types of RAID are out there?* Pridobljeno iz PANDORA: https://pandorafms.com/blog/what-is-raid/

Peltier, T. (2001). *Information Security Policies, Procedures, and Standards*. Pridobljeno iz SRIBD: https://www.scribd.com/document/480658441/Information-Security-Policies-Procedures-and-Standards-Guidelines-for-Effective-Information-Security-Management-PDFDrive

Perhavec, N. (2022). Prehod iz lokalnega IT okolja v oblačno infrastrukturo (trajnost v oblaku/cloud sustainability).

TecnoDigital. (2025). *Razlaga standarda ISO 27001: upravljanje, kontrole in ključi za implementacijo*. Pridobljeno iz ITD: https://informatecdigital.com/sl/kaj-je-standard-ISO-27001/?utm_source=chatgpt.com

Trio. (30. September 2025). *10 Server Security Best Practices Every Admin Should Follow.* Pridobljeno iz Trio: https://www.trio.so/blog/server-security-best-practices

URAD VLADE REPUBLIKE SLOVENIJE. (2025). *Priročnik kibernetske varnosti, Druga dopolnjena izdaja*. Pridobljeno iz https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf

Wikepedia. (n.d). *Good documentation practice*. Pridobljeno iz Wikepedia: https://en.wikipedia.org/wiki/Good_documentation_practice