REPUBLIKA SLOVENIJA
MINISTRSTVO ZA KULTURO

ARHIV REPUBLIKE SLOVENIJE
Zvezdarska 1, 1127 Ljubljana

T: 01 241 42 00
F: 01 241 42 76
E: ars @gov.si
www.arhiv.gov.si

ENOTNE TEHNOLOŠKE ZAHTEVE

II. DEL

ENOTNE TEHNOLOŠKE ZAHTEVE ZA ZAJEM IN HRAMBO GRADIVA V DIGITALNI OBLIKI

Različica 2.1

Ljubljana, 10. julij 2013

Stanje dokumenta

1. Namen dokumenta: **Na podlagi 91. člena ZVDAGA Arhiv RS sprejema enotne tehnološke zahteve, ki podrobneje opredeljujejo poslovne, organizacijske in tehnološke pogoje za izpolnjevanje tega zakona in na njegovi podlagi izdanih podzakonskih predpisov.**

   II. DEL: Enotne tehnološke zahteve za zajem in hrambo gradiva v digitalni obliki

2. Vsebina: **Kazalo vsebine**

3. Oznaka dok.: **ETZ 2.0 – II. del**

4. Številka dokumenta: **382-6/2013/1**

5. Status: **potrjeno**

6. Različica: **2.1**

7. Datum različice: **10. julij 2013**

8. Lastnik: **Ministrstvo za kulturo, Arhiv RS**

9 Avtorji: **projektna skupina za ETZ 2.0 Arhiva RS**

10. Potrdil

	Ime in Priimek	*Datum potrditve*	*Različica*	*Podpis*
Direktor Arhiva RS	***Dr. Dragan Matić***	***6. april 2011***	***2.0***	
Direktor Arhiva RS	***mag.Bojan Cvelfar***	***11. julij 2013***	***2.1***	

11. Dostavljeno: **objava na spletni strani Arhiva RS**

12. Zgodovina različic:

Različica	Datum zadnje spremembe	Izvedene spremembe
0.51	2. februar 2011	*Predlog – objava na internetu za javno obravnavo*
0.52	18. marec 2011	*Dopolnjeno glede na pripombe iz javne obravnave*
2.0	6. april 2011	*Potrjeno s strani direktorja Arhiva RS in objavljeno na spletni strani Arhiva RS*
2.1	10. julij 2013	*Potrjeno s strani v.d. direktorja Arhiva RS in objavljeno na spletni strani Arhiva RS* *Spremembe: Ključne spremembe se nanašajo na vzorčna notranja pravila, ostale spremembe so zaradi večje razumljivosti in pa terminološke. Vse spremembe so prikazane v ločenem dokumentu »Primerjalna tabela med ETZ 2.0 in 2.1«.*

13. Stopnja tajnosti: javno objavljeno

KAZALO VSEBINE

I. SEZNAM ENOTNIH TEHNOLOŠKIH ZAHTEV

1 NOTRANJA PRAVILA IN ORGANIZACIJA

1.1 SPLOŠNO O NOTRANJIH PRAVILIH (v nadaljnjem besedilu NP)

1.1.1 Predhodna priprava na zajem in e-hrambo

ETZ 1.1.1.1 Organizacija mora izvesti predhodno pripravo na zajem in e-hrambo v skladu s predpisi (ZVDAGA, UVDAG, ETZ). Če vloži zahtevek za potrditev NP v državni arhiv, mora k vlogi priložiti poročilo o izvedeni predhodni pripravi na zajem oz. e-hrambo.

Sklic:	

ETZ 1.1.1.2 Poročilo o predhodni pripravi, ki se priloži k vlogi za potrditev NP, mora vključevati najmanj:

- analizo obstoječega stanja upravljanja gradiva:
  - dejavnost organizacije,
  - popis poslovnih in pravnih zahtev (zakonodaja, ki jo mora vlagatelj upoštevati pri zajemu oz. e-hrambi),
  - popisa vrst in virov gradiva, ki nastaja oz. bo zajeto in e-hranjeno;
- zahteve za e-hrambo,
- študijo izvedljivosti,
- načrt e-hrambe.

Sklic:	

Opomba: Če se pripravlja na izvajanje storitve ponudnik, mora biti iz poročila o predhodni pripravi jasno kaj obsega storitev in razmejitev nalog med naročnikom in ponudnikom storitve.

ETZ 1.1.1.3 Organizacija, ki pripravlja vzorčna NP, mora v poročilu o predhodni pripravi (glej ETZ 1.1.1.2) dodatno pojasniti:

- komu so vzorčna NP namenjena,
- katere pogoje mora izpolniti organizacija, ki želi prevzeti ta vzorčna NP.

Opomba: Organizacija, ki želi prevzeti vzorčna NP, naj v okviru predhodne priprave, v skladu z navodili za prevzem vzorčnih NP dodatno preveriti:

- *ali izpolnjuje pogoje za prevzem vzorčnih NP,*
- *ali izbrana vzorčna NP urejajo vsa področja poslovanja, ki jih želi urediti z NP in*
- *ali ji navodila za prevzem omogočajo prilagoditve v obsegu, kot ga načrtuje (glej ETZ 1.1.2.9).*

Sklic:	

1.1.2 Notranja pravila za zajem in e-hrambo

ETZ 1.1.2.1 Organizacija mora na podlagi predhodne priprave sprejeti NP, v katerih mora določiti njihov namen in področja, ki jih urejajo notranja pravila.

Sklic:	

ETZ 1.1.2.2 Organizacija, ki pri državnem arhivu vloži vlogo za potrditev NP, mora priložiti:

- krovni dokument notranjih pravil,
- seznam dokumentov, ki sestavljajo NP vključno s skrbniki teh dokumentov,
- dokumente, iz katerih so NP sestavljena.

Dokumenti NP morajo biti potrjeni (podpisani) s strani pooblaščene osebe v organizaciji.

Opomba: Velja za lastna NP, NP ponudnikov storitev in vzorčna NP.

V krovnem dokumentu NP naj se organizacija sklicuje le na tiste pravne akte oz. priloge, katerih vsebina predstavlja zaključeno celoto in jih v tem dokumentu ni smiselno v celoti zaobjeti. Priloge izven krovnega dokumenta NP so lahko npr.:

- *načrt razvrščanja gradiv po vsebini (klasifikacijski načrt),*
- *načrt za dodeljevanje gradiva v reševanje ter s tem povezanih pravic, nalog in odgovornosti (signirni načrt),*
- *certifikati (npr. ISO 9001, ISO 27001),*
- *varnostna politika (če obstaja certifikat ISO 27001, ni treba prilagati dokumentacije varnostne politike temveč le certifikat in Izjavo o primernosti - angl. Statement of Aplicability),*
- *vzorec pogodbe z zunanjim izvajalcem oz. ponudnikom opreme in storitev hrambe gradiva v digitalni obliki.*

Sklic:	

ETZ 1.1.2.3 Krovni dokument NP in priloge, na katere se NP sklicujejo, morajo biti obvladovani in vsem uporabnikom na voljo, kadar jih potrebujejo. Vzpostavljen mora biti postopek, ki zagotavlja:

- da so vsi dokumenti NP opremljeni z oznako različice in datumom odobritve ter z začetkom veljavnosti,
- da je preprečeno nepooblaščeno spreminjanje dokumentov NP,
- da so NP objavljena na v organizaciji predpisani način in dostopna vsem, ki so jim namenjena,
- da so o spremembah NP obveščeni vsi, katerih delo zadevajo spremembe,da so NP berljiva (uporabna),
- da je preprečena uporaba zastarelih različic NP,
- da so ohranjene stare različice,
- da se NP vzdržujejo, redno pregledujejo in posodabljajo (najmanj enkrat na leto in ob spremembah, ki vplivajo na njihovo vsebino).

Sklic:	

ETZ 1.1.2.4	Organizacija, ki bo predložila NP v potrditev v državni arhiv, mora zahtevku priložiti seznam ETZ tako, da pri vsaki zahtevi izpolni polje »Sklic«. *Opomba: V polju »Sklic« vlagatelj navede dokumentacijo, s katero dokazuje izpolnjevanje zahteve. Navedba mora vključevati: naslov dokumenta, različico dokumenta, številko poglavja ali strani, kjer je odgovor na zahtevo.*
Sklic:	
ETZ 1.1.2.5	Oseba, ki pripravlja vzorčna NP, mora pripraviti navodilo za prevzem vzorčnih NP. Navodilo mora vsebovati najmanj: ▪ opis postopka izvedbe predhodne priprave; ▪ opis postopka prevzema vzorčnih NP z navodili za »personalizacijo«; ▪ določitve dovoljenega obsega prilagoditve določb ali delov določb, ki se nanašajo na status, notranjo organizacijo ali druge notranje lastnosti osebe, ki prevzema vzorčna NP (personalizacija); ▪ opozorilo, da mora prevzemnik vzorčnih NP o prevzemu obvestiti Arhiv RS; ▪ opis aktivnosti, ki jih mora izvesti prevzemnik vzorčnih NP, da ga bo oseba, ki je pripravila vzorčna NP, obveščala o spremembah vzorčnih NP. *Opomba: Zahteva velja za osebe, ki pripravljajo vzorčna NP.*
Sklic:	

Dodatne zahteve za javnopravne osebe in ponudnike:

ETZ 1.1.2.6	*Javnopravna oseba in ponudnik* storitev morata NP obvezno potrditi pri državnem arhivu. Kadar so vzorčna NP namenjena javnopravnim osebam, jih mora vlagatelj obvezno potrditi pri državnem arhivu.
Sklic:	
ETZ 1.1.2.7	*Ponudnik storitev* mora v NP predvideti sistem neodvisnega reševanja sporov pred od ponudnika neodvisno organizacijo.
Sklic:	
ETZ 1.1.2.8	*NP ponudnika spremljevalne storitve zagotavljanja varnih prostorov* morajo vsebovati tudi natančna določila o obsegu posamezne storitve. *Opomba: Obseg varnega prostora je lahko npr. zgolj varni prostor, varni prostor z zagotovljenimi energenti in okoljskimi pogoji, varni prostor in informacijsko-komunikacijska infrastruktura ter podobno).*
Sklic:	

1.1.3 Nadzor nad izvajanjem NP

ETZ 1.1.3.1	Za spremljanje izvajanja NP mora imeti organizacija načrt presoje tega izvajanja.
Sklic:	
ETZ 1.1.3.2	Javnopravne osebe in ponudniki storitev morajo z NP predpisati *zunanjo presojo* izvajanja NP, ki jo mora najmanj enkrat na leto izvesti preizkušen revizor informacijskih sistemov.
Sklic:	
ETZ 1.1.3.3	Za vse organizacije, ki jim je državni arhiv potrdil NP, mora biti predpisana redna notranja presoja izvajanja NP, in sicer najmanj vsaki dve leti. *Opomba: Zahteva ne velja za javnopravne osebe in ponudnike storitev.*
Sklic:	
ETZ 1.1.3.4	Opredeljene morajo biti odgovornosti in način izvajanja notranje oz. zunanje presoje izvajanja NP.
Sklic:	
ETZ 1.1.3.5	O presojah (notranjih in zunanjih) mora obstajati poročilo z vsemi ugotovitvami o izpolnjevanju ali odmiku delovanja od NP. Poročilo mora vsebovati najmanj podatke: ▪ datum in kraj izvedbe presoje, ▪ odgovorne osebe (presojevalci), ▪ namen presoje (načrtovana, ponovna ali izredna presoja), ▪ kateri deli NP so bili presojani (naslov dokumenta (priloge), različica, datum sprejema, odgovorna oseba za sprejem), ▪ ugotovitve, odmiki, dokazila, predlog priporočil in ukrepov za odpravo odmikov pri izvajanju NP, tip ukrepa (preventivni, kurativni), rok izvedbe ukrepa.
Sklic:	
ETZ 1.1.3.6	Če nova NP nadomestijo stara, je treba določiti čas prenehanja slednjih in morebitne izjeme. *Opomba: Zahteva ne velja za prvo različico NP.*
Sklic:	

1.2 NOTRANJA ORGANIZACIJA, VLOGE IN USPOSOBLJENOST OSEBJA

1.2.1 Notranja organizacija

ETZ 1.2.1.1 Organizacija mora imeti v NP določena delovna mesta, ki so povezana z zajemom in e-hrambo. Za ta delovna mesta mora opredeliti splošne, posebne in varnostne pogoje njihove zasedbe.

Sklic:	

ETZ 1.2.1.2 Organizacija mora za vsako delovno mesto, povezano z zajemom in e-hrambo, določiti, do katerih informacijskih virov bo oseba, ki bo opravljala naloge na tem delovnem mestu, pri svojem delu pooblaščeno dostopala.

Sklic:	

ETZ 1.2.1.3 V opisu del in nalog ter opredelitvi odgovornosti zaposlenih morajo biti določene tudi naloge glede varovanja informacij.

Sklic:	

ETZ 1.2.1.4 Organizacija mora, če je le mogoče, zagotoviti takšno razdelitev nalog, ki posamezniku onemogoča neopaženo kompromitiranje ali zlorabo informacij, do katerih ima dostop.

Opomba: Organizacija naj, če je le mogoče glede na njeno organiziranost in skladno z oceno tveganja, oblikuje določbe NP na način, da bo razdelitev nalog takšna, ki bo posamezniku onemogočala neopaženo kompromitiranje ali zlorabo informacij, do katerih ima dostop.

Sklic:	

1.2.2 Usposobljenost zaposlenih, ki delajo z gradivom v digitalni obliki

ETZ 1.2.2.1 Opredeljena mora biti obveznost predhodne usposobljenosti in nadaljnjega izobraževanja zaposlenih, vključno z vzdrževanjem dodatnega strokovnega znanja v obsegu, določenem v ZVDAGA in podrejenih predpisih.

Sklic:	

Dodatni pogoji za zaposlene pri javnopravni osebi in ponudniku storitev

ETZ 1.2.2.2 Javnopravna oseba in ponudnik storitve morata upoštevati dodatne določbe zakonodaje glede izobraževanja zaposlenih.

Opomba: Zdaj to ureja Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb in delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom (Uradi list RS, št. 132/06 in 38/08).

Sklic:	

ETZ 1.2.2.3	Javnopravna oseba in ponudnik morata imeti vzpostavljen sistem rednega, najmanj letnega usposabljanja in izpopolnjevanja zaposlenih, ki delajo na področju, povezanem z zajemom oz. e-hrambo.
Sklic:	
ETZ 1.2.2.4	Vsebina usposabljanj in udeležba zaposlenih na teh usposabljanjih morata biti dokumentirani in shranjeni.
Sklic:	

2 ZAJEM IN E-HRAMBA TER SPREMLJEVALNE STORITVE

2.1 SPLOŠNO O DELOVNIH POSTOPKIH

ETZ 2.1.1.1 Opis vsakega izvajanega delovnega postopka mora vsebovati njegov namen, vhode in izhode, odgovorno osebo, izvajalce in naročnike ter način preverjanja uspešnosti izvedbe z ukrepi za odpravo ugotovljenih napak.

Opomba: Z NP morajo biti opredeljeni delovni postopki ali njihovi deli, ki vplivajo na celovitost in verodostojnost obravnavanega gradiva v digitalni obliki, npr.:

- *pretvorba gradiva iz fizične v digitalno obliko (digitalizacija),*
- *zajem gradiva v digitalni obliki in metapodatkov v informacijski sistem za upravljanje z dokumenti (ISUD),*
- *pretvorba gradiva iz ene v drugo digitalno obliko,*
- *hramba gradiva v digitalni obliki,*
- *urejanje in/ali popisovanje gradiva,*
- *odbiranje arhivskega gradiva iz dokumentarnega gradiva,*
- *izločanje in uničevanje dokumentarnega gradiva.*

Pri najemu zunanjega izvajalca je treba upoštevati zahteve iz poglavja 6.1 Naročanje storitev pri zunanjem izvajalcu.

Sklic:	

2.2 PRIPRAVA NA ZAJEM

2.2.1 Evidentiranje gradiva

ETZ 2.2.1.1 Gradivo mora biti praviloma ob nastanku oz. po prejemu, vendar najpozneje ob zajemu in pretvorbi v digitalno obliko, vpisano v elektronsko evidenco o gradivu oz. v evidenco ISUD na podlagi identifikacijske oznake.

Opomba: Evidenco o gradivu v elektronski obliki oblikujemo ročno ali nastane samodejno z ISUD. Identifikacijska oznaka gradiva je lahko številčna, črkovna ali kombinacija obojega. Identifikacijska oznaka v javni upravi je sestavljena iz klasifikacijskega znaka, zaporedne številke zadeve v okviru tega znaka in letnice nastanka zadeve.

Sklic:	

ETZ 2.2.1.2	*Ponudnik* mora od naročnika pred izvedbo zajema pridobiti evidenco gradiva za zajem ali pa natančna navodila in potrebne (meta)podatke za oblikovanje evidence (popisa gradiva).
Sklic:	
ETZ 2.2.1.3	Evidenca o gradivu mora vsebovati najmanj: ▪ identifikacijski znak, ▪ datum in čas nastanka, ▪ naslov ali kratek opis vsebine gradiva, ▪ avtorja (fizično ali pravno osebo), pošiljatelja ali prejemnika. *Opomba: Pod evidenco se razume evidenca o gradivu ter je lahko npr. dokumentacijski sistem, delovodnik in evidenca prejete oz. odposlane pošte.*
Sklic:	
ETZ 2.2.1.4	Gradivo, pripravljeno za zajem, mora biti pred pretvorbo (iz fizične oz. digitalne oblike) evidentirano in opremljeno z metapodatki. *Opomba:* *Metapodatki se lahko:* - *prenesejo iz obstoječih evidenc o gradivu,* - *prenesejo iz črtnih kod na gradivu,* - *prenesejo z uporabo OCR-programov,* - *vnesejo v ISUD ročno ali pripnejo samodejno.*
Sklic:	

2.2.2 Razvrščanje (klasificiranje) gradiva

ETZ 2.2.2.1	Organizacija mora predpisati postopek razvrščanja gradiva, ki mora temeljiti na načrtu razvrščanja gradiva. *Opomba: Za opis postopka glej ETZ 2.1.1.1.*
Sklic:	
ETZ 2.2.2.2	Določene morajo biti odgovorne osebe za skrbništvo nad načrtom razvrščanja gradiva. *Opomba: Zahteva ne velja za ponudnike storitev.*
Sklic:	

2.2.3 Dodeljevanje gradiva v reševanje oz. dodeljevanje pravic, nalog in odgovornosti (signiranje)

ETZ 2.2.3.1 Organizacija mora predpisati način dodeljevanja gradiva v reševanje ter s tem povezano dodeljevanje pravic, nalog in odgovornosti.

Opomba: V javni upravi na podlagi signirnega načrta skladno z Uredbo o upravnem poslovanju.

Oseba, ki pripravlja vzorčna NP, mora v navodilih za prevzem vzorčnih NP (glej ETZ 1.1.2.5) jasno opredeliti dovoljeni obseg prilagajanja določb, ki so povezane z dodeljevanje pravic, nalog in odgovornosti.

Zahteva ne velja za ponudnike storitev.

Sklic:	

ETZ 2.2.3.2 Določene morajo biti odgovorne osebe za skrbništvo nad načrtom za dodeljevanje gradiva v reševanje oz. dodeljevanje pravic, nalog in odgovornosti (signirni načrt).

Opomba: Zahteva ne velja za ponudnike storitev.

Sklic:	

2.2.4 Roki hrambe

ETZ 2.2.4.1 Gradivu mora biti pred zajemom določen rok hrambe skladno z načrtom razvrščanja gradiva (klasifikacijskim načrtom).

Opomba: Rok hrambe mora biti določen npr. za dosjeje, zadeve in dokumente.

Sklic:	

ETZ 2.2.4.2 *Ponudnik storitve* uničenja gradiva mora od naročnika pridobiti podatke o rokih hrambe za posamezne enote gradiva.

Sklic:	

2.3 ZAJEM GRADIVA

2.3.1 Zahteve za metapodatke

ETZ 2.3.1.1 Organizacija mora z NP opredeliti seznam obveznih metapodatkov za vsako vrsto/tip gradiva in način njihovega vnosa (samodejno, ročno).

Opomba: Ponudnik storitev je dolžan določiti vrste oz. tipe gradiva, za katere opravlja storitev in za vsako vrsto/tip gradiva minimalen nabor metapodatkov, ki jih bo zajemal oz. hranil. Nabor metapodatkov se lahko s pogodbo o izvajanju storitve (glej ETZ 6.1.1.2) razširi.

Sklic:	

ETZ 2.3.1.2	Metapodatki se morajo zajeti (zapisovati in hraniti) v ISUD.
Sklic:	

2.3.2 Oblika zapisa

ETZ 2.3.2.1	Organizacija mora z NP opredeliti veljavne *oblike zapisa*, ki jih uporablja za zajem in e-hrambo posameznih vrst gradiva. *Opomba: Ponudnik storitev je dolžan določiti oblike zapisov v katerih hrani gradivo. Nabor oblik zapisov lahko s pogodbo o izvajanju storitve (glej ETZ 6.1.1.2) razširi s tistimi oblikami zapisov, ki so določene s potrjenimi NP naročnika storitve.*
Sklic:	

2.3.3 Besedilni in mešani dokumenti

ETZ 2.3.3.1	Minimalne zahteve za metapodatke za besedilne dokumente so: ▪ enolična identifikacijska oznaka, ▪ naslov ali kratka oznaka vsebine, ▪ datum (prejetja, nastanka), ▪ avtor oz. pošiljatelj, ▪ naslovnik (prejemnik).
Sklic:	

2.3.4 Film in avdiovizualno gradivo

ETZ 2.3.4.1	Minimalne zahteve za metapodatke za zvočno gradivo so: ▪ enolična identifikacijska oznaka, ▪ naslov, ▪ vsebina, ▪ čas nastanka/datum snemanja, ▪ producent /snemalec, zunanji izvajalec/, ▪ izvorni format, ▪ izvorna dolžina /čas/, ▪ vrsta nosilca. *Opomba: Glede na vrsto zvočnega gradiva so mogoči še drugi metapodatki, npr. producent, izvorni jezik.*
Sklic:	

ETZ 2.3.4.2	Minimalne zahteve za metapodatke za film in avdiovizualno gradivo so: ▪ enolična identifikacijska oznaka, ▪ naslov, ▪ leto nastanka, ▪ izvorni format, ▪ izvorni nosilec, ▪ izvorni jezik.
Sklic:	

2.3.5 Spletne strani

ETZ 2.3.5.1	Organizacija mora oceniti in ovrednotiti potrebe po zajemu in e-hrambi spletnih dokumentov na svojih spletnih mestih (intranet, ekstranet, javno spletišče ipd.). *Opomba: Zahteva ne velja za ponudnike storitev.*
Sklic:	
ETZ 2.3.5.2	Organizacija mora na podlagi načrta razvrstitve gradiva (klasifikacijskega načrta) in ocene iz prejšnje zahteve (ETZ 2.2.5.1) narediti *seznam spletnih dokumentov* (ali sklopov ali spletnih mest) za zajem. *Opomba: Zahteva ne velja za ponudnike storitev.*
Sklic:	
ETZ 2.3.5.3	Za vsako vrsto dokumenta (ali skupine enakovrednih spletnih dokumentov) s seznama spletnih dokumentov je treba v zvezi z zajemom določiti: ▪ izvor, ▪ mesto objave, ▪ obliko, ▪ pogostost zajema, ▪ postopek zajema in e-hrambe, ▪ obseg potrebnih metapodatkov, ▪ seznam funkcionalnosti, ki se ob zajemu in e-hrambi ohranjajo, in ▪ odgovorne osebe.
Sklic:	

ETZ 2.3.5.4	Organizacija mora zagotoviti, da so vsi spletni dokumenti, predvideni za e-hrambo, zajeti v ISUD. Pri tem morajo biti *poleg vsebine spletnih* dokumentov zajeti metapodatki: ▪ enolična identifikacijska oznaka (evidenčna oznaka), ▪ predmet (zadeva), ▪ sestava, ▪ kontekst dokumenta in mesto objave (npr. URL[1]), ▪ identifikator dokumenta (npr. URN[2]).
Sklic:	
ETZ 2.3.5.5	Spletni dokumenti ali njihovi deli, ki vključujejo besedilno vsebino in predstavljajo besedilni del teh dokumentov, morajo biti v eni od oblik zapisa za spletne dokumente in preverjeni z ustreznim orodjem.
Sklic:	
ETZ 2.3.5.6	Opredeljena morata biti oblika in obseg spletnih dokumentov, ki bosta poleg ohranjanja vsebine omogočala kar največjo stopnjo ohranjanja prikaza, funkcionalnosti in zgradbe, vendar skladno z namenom e-hrambe.
Sklic:	

2.3.6 Elektronska pošta

ETZ 2.3.6.1	Organizacija mora oceniti in ovrednotiti potrebe po zajemu in e-hrambi elektronske pošte, in sicer: ▪ vhodnih dokumentov v e-poštni predal, ▪ izhodnih dokumentov iz e-poštnega predala, ▪ e-poštnih predalov. *Opomba: Zahteva ne velja za ponudnike storitev.*
Sklic:	
ETZ 2.3.6.2	Organizacija mora na podlagi načrta za razvrščanje (klasifikacijski načrt) in ocene iz prejšnje zahteve (ETZ 2.2.6.1) določiti in izdelati seznam e-poštnih predalov oz. dokumentov, ki jih je treba zajemati in shranjevati. Treba je določiti: ▪ enolično identifikacijsko oznako (evidenčna oznaka), ▪ izvor (e-poštni predal), ▪ obliko zapisa e-hrambe, ▪ način zajema, ▪ obseg potrebnih metapodatkov, ▪ odgovorne osebe.
Sklic:	

[1] URL: Uniform Resource Locators (naslov spletne strani).

[2] URN: Uniform Resource Name. Enolično in trajno označuje objekt, z njim pridemo do želenega objekta tudi, če se spremeni naslov spletne strani ali lokacija objekta.

ETZ 2.3.6.3	Organizacija mora zagotoviti, da so vsi dokumenti e-pošte, za katere se predvideva e-hramba, zajeti v ISUD. Pri tem morajo biti poleg vsebine zajeti metapodatki iz razširjenega zaglavja (angl. *header*). *Opomba:* *Iz razširjenega zaglavja morajo biti zajeti najmanj:* - *naslov poštnega predala prejemnika odgovorov (polje »From« v glavi sporočila),* - *naslov poštnega predala pošiljatelja e-sporočila (polje »Sender« v glavi sporočila),* - *naslov prejemnika e-sporočila (polje »To« v glavi sporočila),* - *naslov/predmet e-sporočila (polje »Subject« v glavi sporočila),* - *datum e-sporočila (polje »Date« v glavi sporočila),* - *identifikator e-sporočila (polje »Message-ID« v glavi sporočila),* - *število priponk,* - *za vsako priponko identifikator osnovnega elektronskega sporočila,* - *zastavica, da je bil dokument spremenjen,* - *informacija o prikrivalnem postopku (enkripciji),* - *informacija o elektronskem podpisu,* - *poštni predal, iz katerega je bil narejen zajem (npr. poslano, prejeto, oseba NN…).*
Sklic:	

2.3.7 Podatkovne zbirke in uradne evidence

Skupne zahteve za podatkovne zbirke in uradne evidence javnopravnih oseb:

ETZ 2.3.7.1	Vsaka podatkovna zbirka oz. uradna evidenca mora biti dokumentirana najmanj z: ▪ opisom tehničnega okolja, ▪ opisom strukture podatkov, kar vključuje tudi podatkovni model, vire podatkov in šifrante, ▪ opisom uporabljanega izrazoslovja (semantike), tako da bo mogoče zagotoviti uporabo podatkov iz podatkovne zbirke oz. uradne evidence tudi zunaj okolja, v katerem so nastali.
Sklic:	
ETZ 2.3.7.2	Spremembe tehničnega okolja, strukture podatkov, vključno s podatkovnim modelom, morajo biti dokumentirane in zagotavljati e-hrambo najmanj s/z: ▪ specifikacijo sprememb, ▪ načrtom izvedbe sprememb (vključuje tudi načrt preizkušanja in preverjanja celovitosti in pravilnosti prenosa), ▪ utemeljitvijo upravičenosti morebitnega brisanja ali opustitve prenosa izbranih podatkov, ▪ dokumentiranim dokazilom o izvedbi skladno z načrtom. *Opomba: Glej tudi poglavje 5.1.1.1 Upravljanje s spremembami*
Sklic:	

Dodatne zahteve za uradne evidence:

ETZ 2.3.7.3	Za uradne evidence morajo biti dokumentirane vse spremembe vrednosti podatkov (atributov). *Opomba: Če se vrednost podatka spremeni, mora biti stara vrednost ohranjena tako, da je vedno mogoč vpogled v staro stanje na določen datum. Pristojni arhiv lahko s strokovnimi navodili za odbiranje omeji izbor entitet, za katere je treba voditi vse spremembe njihovih vrednosti (atributov).*
Sklic:	
ETZ 2.3.7.4	Upravljavec uradne evidence mora voditi vso dokumentacijo o upravljanju evidence in se nanaša najmanj na: ▪ zahteve iz ETZ 2.3.7.1 in 2.3.7.2, ▪ pravne podlage, ▪ vire podatkov, ▪ odgovorne osebe.
Sklic:	
ETZ 2.3.7.5	Kadar spremembe tehničnega okolja oz. podatkovnega modela vplivajo na entitete ali atribute v uradni evidenci oz. metapodatke, mora upravljavec pisno obvestiti pristojni arhiv o nameravanih spremembah najmanj 14 delovnih dni pred njihovo uveljavitvijo, da pridobi dodatna navodila.
Sklic:	
ETZ 2.3.7.6	Dokumentacija o pravnih podlagah za upravljanje uradnih evidenc mora obsegati vse javne in interne predpise, ki urejajo to upravljanje, vključno s spremembami.
Sklic:	
ETZ 2.3.7.7	Za posamezno uradno evidenco morajo biti dokumentirani vsi viri podatkov na ravni vpisnih polj uporabniškega vmesnika za vnos oz. spremembo podatkov v evidenco.
Sklic:	
ETZ 2.3.7.8	Upravljavec uradne evidence mora o vseh spremembah strukture podatkov v enem mesecu po uveljavitvi spremembe obvestiti pristojni arhiv. *Opomba: Namen je dopolnitev pisnega strokovnega navodila za odbiranje arhivskega gradiva iz dokumentarnega ali dodatnih navodil.*
Sklic:	

2.4 PRETVORBA GRADIVA V OBLIKO ZA DOLGOROČNO E-HRAMBO

ETZ 2.4.1.1 Če v organizaciji obstaja potreba po pretvorbi gradiva v obliko za dolgoročno e-hrambo, morajo NP opredeljevati:

- odgovorno osebo za izvedbo pretvorbe in njene naloge v povezavi s tem,
- oblike zapisa, ki jih organizacija določi za dolgoročno e-hrambo,
- merila in preverjanje pravilnosti (ustreznosti) pretvorbe gradiva,
- ukrepe ob ugotovljenih nepravilnostih.

Opomba: Glej tudi ETZ 2.1.1.1.

Naloge odgovorne osebe za izvedbo pretvorbe vključujejo najmanj:

- *spremljanje veljavne oblike zapisa za dolgoročno hrambo,*
- *določitev obsega gradiva za pretvorbo,*
- *skrb za pravočasno in pravilno pretvorbo gradiva v novo obliko zapisa.*
- *dokumentiranje pretvorbe.*

Kadar izvaja pretvorbo gradiva v obliko za dolgoročno hrambo ponudnik storitve, mora naročnik storitve v svojih NP določiti odgovorno osebo, ki sodeluje z izvajalcem in je na stani naročnika odgovorna za pravočasnost in ustreznost pretvorbe. Ponudnik mora v svojih NP predvideti sodelovanje z odgovorno osebo pri naročniku.

Sklic:	

2.5 DOLGOROČNA E-HRAMBA IN ZAVAROVANJE SHRANJENEGA GRADIVA PRED IZGUBO

2.5.1 Zagotavljanje avtentičnosti in celovitosti gradiva

ETZ 2.5.1.1 Organizacija mora zagotoviti in z NP opredeliti ustrezna **osnovna tehnološka sredstva** za vzdrževanje celovitosti in avtentičnosti gradiva za celotno obdobje hrambe gradiva v digitalni obliki.

Opomba: Osnovna tehnološka sredstva so tista, ki ne temeljijo na kriptografskih mehanizmih ali ne podpirajo dolgoročnega vzdrževanja veljavnosti varnostnih vsebin za dokazovanje celovitosti in avtentičnosti. Takšna sredstva so npr. prstni odtis, elektronski podpis in časovni žig.

Sklic:	

ETZ 2.5.1.2 Organizacija, ki upravlja dokumentarno in arhivsko gradivo, izvorno nastalo v digitalni obliki, ki pred zajemom že vključuje varnostne vsebine, mora zagotoviti in z NP opredeliti ustrezna **napredna tehnološka sredstva** za vzdrževanje veljavnosti že obstoječih varnostnih vsebin.

Opomba: Z vzdrževanjem veljavnosti obstoječih varnostnih vsebin dokazujemo celovitost in avtentičnost gradiva za celotno obdobje njegove hrambe.

Sklic:	

ETZ 2.5.1.3	Organizacija mora z organizacijskimi ukrepi opredeliti način uporabe tehnoloških sredstev za zagotavljanje celovitosti in avtentičnosti gradiva. *Opomba: Pri uporabi osnovnih tehnoloških sredstev mora organizacija opredeliti tudi dodatne (komplementarne) organizacijske ukrepe, ki zagotavljajo varno in zanesljivo uporabo sredstev za zagotavljanje celovitosti in avtentičnosti.*
Sklic:	
ETZ 2.5.1.4	Organizacija, ki zajema in hrani dokumentarno in arhivsko gradivo, izvorno nastalo v digitalni obliki, mora ob zajemu gradiva, ki vsebuje elektronski podpis, preveriti njegovo veljavnost in podatek o preverjanju veljavnosti dodati kot metapodatek dokumentu. Veljavnost e-podpisa se v nadaljnjih rokovanjih z gradivom ne preverja več (npr. ob pretvorbi iz enega formata v drugega).
Sklic:	
ETZ 2.5.1.5	Organizacija, ki hrani gradivo, izvorno nastalo v digitalni obliki in s pridobljenim statusom arhivskega gradiva, mora ob izročitvi tega gradiva v pristojni arhiv predložiti tudi pripadajoče varnostne vsebine, ki so pripravljene na podlagi naprednih tehnoloških sredstev.
Sklic:	

Dodatne zahteve za javnopravne osebe in ponudnike storitev e-hrambe

ETZ 2.5.1.6	Javni arhivi in javnopravne osebe, ki imajo dovoljenje za lastno varstvo arhivskega gradiva (62. člen ZVDAGA), in ki hranijo arhivsko gradivo v digitalni obliki morajo zagotoviti ustrezna napredna tehnološka sredstva za vzdrževanje celovitosti in avtentičnosti tega gradiva. *Opomba: Tehnološki prijemi nadomeščajo organizacijske ukrepe za zagotavljanje celovitosti in avtentičnosti dokumentarnega gradiva. Šibkejša ko so sredstva za vzdrževanje celovitosti in avtentičnosti, kompleksnejši so organizacijski ukrepi. Za izpolnjevanje osnovnih zahtev za prenosljivost gradiva pri e-hrambi so tehnološki prijemi edina ustrezna sredstva za vzdrževanje celovitosti in avtentičnosti pri prehodu med informacijskimi sistemi za e-hrambo. Vse organizacije torej, katerih postopki vključujejo prenos gradiva med sistemi e-hrambe in e-arhiviranja, morajo uporabljati izključno napredna tehnološka sredstva za zagotavljanje celovitosti in avtentičnosti, ki so neodvisna od posebne programske opreme (ISUD). Uporabljena sredstva morajo biti navedena v ETZ oz. morajo delovati v skladu z mednarodno predpisanimi tehnološkimi priporočili.*
Sklic:	
ETZ 2.5.1.7	Ponudnik storitev mora uporabljati napredna tehnološka sredstva za zagotavljanje celovitosti in avtentičnosti tako, da so prenosljiva med sistemi. *Opomba: Ponudnik storitve e-hrambe mora kadar koli med hrambo zagotoviti prenosljivost gradiva med informacijskimi sistemi. Hkrati mora zagotoviti prenosljivost varnostnih vsebin. Slednje morajo biti ustvarjene tako, da so tehnološko neodvisno*

preverljive in da je mogoče v ciljnem sistemu zagotoviti njihovo nadaljnje vzdrževanje. Varnostne vsebine morajo temeljiti na naprednih tehnoloških sredstvih. V NP mora ponudnik storitve e-hrambe opredeliti, kako bo te vsebine skupaj z gradivom izvozil iz svojega sistema.

Sklic:	

2.5.2 Neprekinjeno poslovanje

Izdelava, hramba in uporaba varnostnih kopij gradiva v digitalni obliki

ETZ 2.5.2.1 Organizacija mora zaradi zavarovanja gradiva pred izgubo oz. poškodovanjem opredeliti način izdelave **varnostnih kopij** tega gradiva v digitalni obliki.

Opomba: Pogostost izdelave varnostnih kopij se določi na podlagi ocene tveganja.

Sklic:	

ETZ 2.5.2.2 Organizacija mora na oddaljenem mestu (sekundarna lokacija) poleg varnostne kopije gradiva shraniti še druge podatke (npr. kopijo aplikativne programske opreme in pripadajoča navodila), potrebne za obnovo e-hranjenega gradiva.

Sklic:	

ETZ 2.5.2.3 Varnostne kopije gradiva mora organizacija shraniti na oddaljenem mestu, ki je od glavnega (primarnega) mesta hrambe oddaljeno najmanj 30 km zračne črte.

Sklic:	

ETZ 2.5.2.4 Organizacija mora imeti vzpostavljen postopek prenosa varnostnih kopij na oddaljeno mesto in za to določene odgovorne osebe.

Sklic:	

ETZ 2.5.2.5 Organizacija mora imeti izdelan **načrt za obnovo podatkov in** določiti njegovega **skrbnika.** Ta načrt mora vključevati najmanj te podatke:

- kdo in kako lahko pride do varnostnih kopij na oddaljenih mestih,
- postopek vzpostavitve sistema,
- postopek uporabe varnostnih kopij pri morebitni potrebi po restavriranju gradiva,
- postopek brisanja zastarelih kopij in uničevanja izrabljenih nosilcev, na katerih so bile shranjene kopije gradiva,
- navodilo o obveznem dokumentiranju in hrambi te dokumentacije pri izvedbi postopka obnove podatkov.

Sklic:	

ETZ 2.5.2.6 Organizacija mora načrt za obnovo podatkov preizkusiti najmanj enkrat na leto.

Sklic:	

Dodatne zahteve za javnopravne osebe in ponudnike storitev e-hrambe

ETZ 2.5.2.7	Javnopravna oseba oz. ponudnik storitve e-hrambe, ki hrani javno arhivsko gradivo v digitalni obliki, mora zagotoviti shranjevanje varnostnih kopij gradiva in podatkov, potrebnih za obnovo sistema e-hrambe, na najmanj dveh geografsko oddaljenih mestih, ki morata biti medsebojno in od glavnega mesta hrambe (primarne lokacije) oddaljeni najmanj 30 km zračne črte.
Sklic:	
ETZ 2.5.2.8	Kadar javnopravna oseba ali ponudnik storitve e-hrambe hrani arhivsko gradivo, mora imeti poleg načrta za obnovo podatkov izdelan **načrt neprekinjenega delovanja** (poslovanja) e-hrambe**.**
Sklic:	

ETZ 2.5.2.9	Načrt neprekinjenega delovanja e-hrambe mora vključevati najmanj: ▪ podatke o glavnem (primarnem) in oddaljenih (sekundarnih) mestih hrambe (organizacija, naslov, kraj, telefon), ▪ pravila dostopa do glavnega in oddaljenih mest hrambe, ▪ opis oddaljenih mest: prostor, komunikacijske povezave (telefon, internet, e-pošta), uvedeni fizični in tehnični ukrepi (vgrajeni senzorji gibanja, alarmni sistem, protipožarni senzorji, protivlomna vrata, videonadzor), če je v prostoru nameščena strojna in programska oprema, njen opis in v kakšnem delujočem stanju je, ▪ osnovne podatke o odgovornih osebah v kriznem položaju in njihove podatke za stik (ime in priimek, telefon v službi in doma, GSM, e-pošta), ▪ podatke o zunanjih javnih službah nujne pomoči (gasilci, reševalci, policija, zavarovalnica) in njihove podatke za stik, ▪ navedene kritične poslovne procese oz. naloge, ki so razvrščene (rangirane) po nujnosti vzpostavitve za delovanje organizacije, in akcijski načrt za njihovo vzpostavitev, ▪ seznam ključnih dobaviteljev in pogodbenikov ter njihove podatke za stik, ▪ način obravnavanja načrta neprekinjenega delovanja med zaposlenimi (interni sestanki, interno usposabljanje, simulacije izrednih dogodkov najmanj enkrat na leto), ▪ način komuniciranja s sodelavci pri izrednem dogodku (osebno, telefon, e-pošta), ▪ način komuniciranja s poslovnimi partnerji pri izrednem dogodku (osebno, elektronska pošta, GSM, telefon), ▪ podatke o varnostnih kopijah (odgovorna oseba, mesto hranjenja varnostnih kopij, ravnanje pri uničenju oz. poškodovanju podatkov na glavnem mestu hrambe), ▪ podatke za stik z zaposlenimi v nujnih primerih in področje odgovornosti, ▪ načine ukrepanja pri izrednih dogodkih in scenarije okrevanja, ▪ načrt vzpostavitve normalnega stanja sistema, kakršen je bil pred katastrofo, ▪ načrt izobraževanja in usposabljanja zaposlenih v zvezi z načrtom neprekinjenega delovanja, ▪ načrt preverjanja načrta neprekinjenega delovanja (odgovorne osebe, časovna opredelitev).
Sklic:	
ETZ 2.5.2.10	Ponudnik storitve e-hrambe mora poleg varnostne kopije gradiva in drugih podatkov, potrebnih za obnovo e-hranjenega gradiva, na oddaljenem mestu hrambe zagotoviti tudi tako nadomestno informacijsko infrastrukturo sistema za e-hrambo, katere razpoložljivost mora omogočati, da bo naročniku e-hrambe v obdobju iz pogodbe, ki jo je sklenil z njim, zagotovil pogodbeni obseg shranjevanja oz. dostopa do shranjenega gradiva.
Sklic:	
ETZ 2.5.2.11	Načrt neprekinjenega delovanja mora biti najmanj enkrat na leto celovito preizkušen.
Sklic:	

ETZ 2.5.2.12	Načrt neprekinjenega delovanja mora biti posodobljen ob vsaki organizacijski spremembi, zamenjavi osebja ali večji spremembi v informacijskem sistemu, ki vpliva nanj. V tem primeru mora biti načrt ponovno preizkušen v primernem obsegu.
Sklic:	
ETZ 2.5.2.13	Vsi zaposleni, vključeni v izvajanje dejavnosti iz načrta neprekinjenega delovanja, morajo biti ustrezno usposobljeni ter celovito seznanjeni s svojimi vlogami in odgovornostmi, vezanimi na to izvajanje.
Sklic:	
ETZ 2.5.2.14	Pri uporabi načrta neprekinjenega delovanja morajo biti vsi izvedeni postopki natančno dokumentirani in shranjeni.
Sklic:	

2.6 ODBIRANJE IN IZROČANJE ARHIVSKEGA GRADIVA V DIGITALNI OBLIKI TER SODELOVANJE S PRISTOJNIM ARHIVOM

ETZ 2.6.1.1	Ustvarjalec javnega arhivskega gradiva mora pristojnemu arhivu izročiti gradivo v takšni obliki, na takšnem nosilcu in s tistimi metapodatki, ki jih je s strokovnim navodilom določil pristojni arhiv. *Opomba: Glej tudi ETZ 2.1.1.1.*
Sklic:	

2.7 IZLOČANJE IN UNIČEVANJE DOKUMENTARNEGA GRADIVA

ETZ 2.7.1.1	Opredeljen mora biti postopek vključno z merili, po katerih se izvaja izločanje in uničevanje gradiva. *Opomba: Glej tudi ETZ 2.1.1.1.* *Izloča se dokumentarno gradivo, ki so mu potekli roki hrambe.*
Sklic:	
ETZ 2.7.1.2	Določene morajo biti odgovorne osebe, ki izvajajo postopek uničevanja gradiva. *Opomba: Uničevanje gradiva izvaja komisija, ki jo določi predstojnik. Pri javnopravnih osebah mora biti sestavljena iz treh članov.*
Sklic:	

ETZ 2.7.1.3	Izvedba postopka uničevanja gradiva mora biti dokumentirana: a) z zapisnikom komisije za uničenje gradiva, ki mora obsegati: ▪ čas in kraj uničenja, ▪ osebe, ki odgovarjajo za pravilno izvedbo postopka, ▪ osebe (ali ponudniki storitev), ki so izvedle uničenje; b) s seznamom uničenega gradiva (priloga k zapisniku).
Sklic:	
ETZ 2.7.1.4	Zapisnik o uničenju gradiva vključno s seznamom uničenega gradiva se hrani trajno. *Opomba: Javnopravne osebe morajo ohraniti tudi vse evidence o dokumentarnem gradivu, ne glede na to, ali je bilo vanje vključeno tudi uničeno gradivo.*
Sklic:	

3 INFORMACIJSKA VARNOST

3.1 POPIS IN VARNOSTNA RAZVRSTITEV INFORMACIJSKIH VIROV

3.1.1 Popis informacijskih virov

ETZ 3.1.1.1	Organizacija mora izdelati in vzdrževati seznam vseh pomembnih informacijskih virov, ki so vključeni v zajem in e-hrambo ter evidenco zajetega oz. hranjenega gradiva. *Opomba: Glej tudi ETZ 4.2.1.1 in ETZ 4.4.2.4.*
Sklic:	

3.1.2 Odgovorne osebe za varovanje informacijskih virov

ETZ 3.1.2.1	Organizacija mora določiti skrbnike posameznih informacijskih virov oz. skupin virov, ki so odgovorni za uporabo oz. obravnavanje virov v skladu s predpisanimi oz. pogodbeno določenimi zahtevami, pravili in standardi.
Sklic:	

3.1.3 Varnostna razvrstitev informacijskih virov

ETZ 3.1.3.1 Informacijski vir, ki vsebuje zaupne podatke, mora biti v skladu z oceno tveganja in svojo kritičnostjo oz. občutljivostjo varnostno razvrščen ter označen v skladu s predpisi in notranjimi akti, ki urejajo upravljanje, obdelavo in uporabo posameznih kategorij zaupnih podatkov.

Opomba: Med zaupne podatke sodijo npr. osebni podatki, poslovne skrivnosti, bančna, davčna, statistična in izpitna tajnost. Npr. gradivo s tajnimi podatki, ki jim je bila tajnost določena na podlagi določb Zakona o tajnih podatkih (ZTP) in predpisov, izdanih na njegovi podlagi, mora biti varnostno razvrščeno in označeno s stopnjami tajnosti ter drugimi predpisanimi oznakami v skladu z ZTP.

Sklic:	

3.2 ORGANIZIRANJE INFORMACIJSKE VARNOSTI

3.2.1 Ocena tveganja

ETZ 3.2.1.1 Organizacija mora izdelati **oceno tveganja**, s katero prepoznava in obvladuje tveganje, povezano s človeškimi viri, ter pravno, poslovno, organizacijsko, okoljsko in tehnološko tveganje, vezano na zajem oz. e-hrambo gradiva. Če organizacija vloži zahtevek za potrditev NP v državni arhiv, mora k vlogi priložiti tudi poročilo o izvedeni oceni tveganja.

Sklic:	

ETZ 3.2.1.2 Ocena tveganja mora temeljiti na dokumentirani metodologiji.

Sklic:	

ETZ 3.2.1.3 Ocena tveganja mora biti najmanj enkrat na leto in ob spremembah, ki vplivajo na tveganje, posodobljena tako, da izraža dejansko stanje. Enako velja za izbrana nadzorstva (ukrepe), ki izhajajo iz ocene tveganja.

Sklic:	

3.2.2 Notranje pravna ureditev informacijske varnosti

ETZ 3.2.2.1 Organizacija mora pri pripravi in sprejemu NP v formalni notranje pravni obliki določiti ukrepe in postopke informacijske varnosti (**politika informacijske varnosti** kot del NP), bistvene za zajem oz. e-hrambo gradiva, pa tudi način upravljanja, izvajanja in nadziranja ukrepov ter postopkov informacijske varnosti.

Sklic:	

ETZ 3.2.2.2	Organizacija mora imenovati **odgovorno osebo za informacijsko varnost** (vodja informacijske varnosti) in ji določiti pristojnosti oz. naloge varovanja zajema oz. e-hrambe.
Sklic:	
ETZ 3.2.2.3	Zaposleni v organizaciji (redno in začasno) in morebitni zunanji sodelavci morajo podpisati izjavo o zaupnosti oz. varovanju informacij.
Sklic:	

Dodatne zahteve za javnopravne osebe in ponudnike storitev

ETZ 3.2.2.4	Javnopravna oseba in ponudnik storitve zajema oz. e-hrambe morata poleg izpolnitve zahtev iz poglavij 3.1.2.1 in 3.1.2.2 vzpostaviti tudi **sistem upravljanja informacijske varnosti** (SUIV), katerega dokumentacija mora obsegati še: ▪ določitev obsega in meje sistema informacijske varnosti, vezano na zajem oz. e-hrambo; ▪ izjavo vodstva o zavezanosti, da bo zagotavljalo potrebne vire za dosego ciljev; ▪ dokumentirana dokazila o izvajanju varnostnih ukrepov in postopkov.
Sklic:	

3.3 FIZIČNO IN TEHNIČNO VAROVANJE PROSTOROV IN OPREME

3.3.1 Določitev prostorov za zajem in e-hrambo ter njihovo varovanje

ETZ 3.3.1.1	Organizacija mora določiti prostore za zagotovitev varnega izvajanja zajema in e-hrambe (varovano območje) v skladu s pomembnostjo informacijskih virov (gradiva in opreme), ki so na tem območju.
Sklic:	
ETZ 3.3.1.2	Organizacija mora za varovana območja določiti in izvesti varnostne ukrepe ter postopke za zaščito pred nepooblaščenim dostopom in okoljskimi nevarnostmi (požar, izlitje ali vdor vode, nenadne spremembe temperature ali vlage, dim, prah in podobno). *Opomba: Varnostni ukrepi morajo izhajati iz ugotovitev ocene tveganja ter upoštevati varnostno razvrstitev informacijskih virov in morebitne posebne zahteve predpisov, ki urejajo varovanje določenih kategorij podatkov oz. gradiva. Vsi varnostni ukrepi in postopki morajo delovati v vsakem trenutku (tudi zunaj delovnega časa).*
Sklic:	

3.3.2 Varovanje vstopanja v prostore za zajem in e-hrambo

ETZ 3.3.2.1 Organizacija mora sprejeti in upoštevati pravila vstopanja v prostore, v katerih se izvaja zajem ali e-hramba (varovana območja), ki morajo veljati za zaposlene in za druge osebe.

Opomba: Pri urejanju pravil vstopanja in gibanja na varovana območja je treba upoštevati tudi druge veljavne predpise, še posebno Zakon o varstvu osebnih podatkov in Zakon o tajnih podatkih.

Sklic:	

ETZ 3.3.2.2 Vstop zaposlenih in drugih oseb na varovano območje mora biti evidentiran, zapisi pa redno pregledovani s strani odgovorne osebe za posamezno varovano območje skladno z oceno tveganja.

Sklic:	

3.4 UPRAVLJANJE DOSTOPNIH PRAVIC DO SISTEMA IN GRADIVA

3.4.1 Postopek dodelitve, spreminjanja in odvzema dostopnih pravic uporabnikov

ETZ 3.4.1.1 Organizacija mora imeti opredeljena pravila za dodeljevanje uporabniških imen s pripadajočimi gesli oz. drugih identifikatorjev. Zagotovljena mora biti enolična identifikacija vseh uporabnikov.

Opomba: Med druge identifikatorje spadajo npr. pametne kartice z digitalnimi potrdili, generatorji žetonov za enkratno prijavo, biometrični podatki.

Sklic:	

ETZ 3.4.1.2 Če organizacija uporablja gesla, mora imeti postavljena pravila za njihovo upravljanje, ki morajo obsegati najmanj:

- obvezno sestavo gesel,
- časovno opredelitev in postopek za redno spreminjanje gesel ter
- postopek za prvo in po potrebi nadaljnjo dostavo gesel uporabnikom.

Sklic:	

ETZ 3.4.1.3 Organizacija mora imeti opredeljen in dokumentiran postopek in odgovorne osebe za upravljanje dostopnih pravic (dodelitev, spreminjanje oz. odvzem). Postopek mora veljati tudi pri premestitvi zaposlenega na dela z drugačnimi pristojnostmi/odgovornostmi ali prenehanju zaposlitve oz. sodelovanja.

Opomba: Pri dodeljevanju dostopnih pravic je treba upoštevati tudi pogoje oz. zahteve za dostop do podatkov, ki jih vsebuje shranjeno gradivo, in pogoje, ki jih določajo drugi ustrezni predpisi, še posebno Zakon o varstvu osebnih podatkov in Zakon o tajnih podatkih.

Sklic:	

ETZ 3.4.1.4	Odgovorne osebe za upravljanje dostopnih pravic morajo voditi sprotno evidenco njihovega upravljanja, v katero morajo biti vključeni najmanj: ▪ zahtevki za dodelitev oz. odvzem uporabniških pravic, ▪ seznam dostopnih pravic do sistemov za posamezne uporabnike.
Sklic:	
ETZ 3.4.1.5	Vzpostavljen mora biti nadzor nad dostopi do informacijskega sistema in gradiva (formalni postopek pregledovanja uporabniških pravic dostopa).
Sklic:	

3.5 REVIZIJSKE SLEDI

3.5.1 Vrste revizijskih sledi, vezanih na dostop do gradiva

ETZ 3.5.1.1	Organizacija mora za vse vrste e-hranjenega gradiva določiti obseg zapisovanja revizijske sledi in rok njene hrambe. *Opomba: Obseg revizijske sledi naj bi zajemal vsaj kdaj, kdo, do katerega vira in kakšne spremembe je izvajal. Pri tem je treba izhajati tudi iz ocene tveganja in področne zakonodaje.*
Sklic:	
ETZ 3.5.1.2	Organizacija mora določiti: ▪ skrbnika z odgovornostjo upravljanja revizijskih sledi (nastavitve, način obdelave in uporabe), ▪ osebe, ki so pooblaščene za dostop do zapisov revizijskih sledi.
Sklic:	

3.5.2 Revizijske sledi, vezane na dostop do informacijskega sistema za e-hrambo

ETZ 3.5.2.1	Organizacija mora za dostope do informacijskega sistema za e-hrambo določiti obseg revizijske sledi, vključno z načinom uporabe in rokom hrambe. *Opomba: Obseg revizijske sledi naj bi zajemal vsaj kdaj, kdo in kakšno spremembo je izvedel na posameznih virih (dokumentih, strežnikih, uporabniških pravicah,..).*
Sklic:	

3.6 UPRAVLJANJE VARNOSTNIH INCIDENTOV

ETZ 3.6.1.1 Organizacija mora določiti postopek in odgovorno osebo za upravljanje varnostnih incidentov. Postopek mora vključevati zavarovanje in hrambo revizijskih ter drugih sledi, ki bi bile lahko uporabne v postopkih, vezanih na varnostni incident.

Opomba: Upravljanje varnostnih incidentov zajema njihovo zaznavanje, obravnavanje, dokumentiranje in analiziranje.

Sklic:	

ETZ 3.6.1.2 Organizacija mora voditi evidenco varnostnih incidentov in določiti njenega skrbnika. Ta evidenca mora vključevati najmanj:

- vrsto incidenta,
- datum, čas in kraj incidenta,
- vzrok incidenta,
- izvedene ukrepe v zvezi z incidentom (kdo, kdaj in kako je ukrepal).

Sklic:	

ETZ 3.6.1.3 *Ponudnik storitev* mora v svojih NP predvideti možnost, da bo naročnik dostopal in pregledoval statistiko ali zapise napak, nastalih pri izvajanju storitev.

Sklic:	

4 INFORMACIJSKA OPREMA IN INFRASTRUKTURA

4.1 ELEKTRIČNA IN TELEKOMUNIKACIJSKA NAPELJAVA

ETZ 4.1.1.1 Električna in telekomunikacijska napeljava morata biti izvedeni tako, da ju ni mogoče nenamerno prekiniti ali brez večjih težav uničiti ali zlorabiti.

Opomba: Zahteva mora biti opredeljena z NP, ni pa predmet presoje NP temveč samo predmet preverjanja izvajanja NP.

Sklic:	

4.2 STROJNA OPREMA

ETZ 4.2.1.1 Organizacija mora v NP navesti vsaj te podatke o strojni opremi:

- tip strojne opreme,
- proizvajalec,
- serija oz. model.

Opomba: Glej tudi ETZ 3.1.1.1.

Sklic:	

ETZ 4.2.1.2	Strojna oprema mora biti skladna z mednarodnimi, državnimi in drugimi splošno priznanimi standardi.
Sklic:	
ETZ 4.2.1.3	Strojna oprema mora biti mednarodno uveljavljena.
Sklic:	
ETZ 4.2.1.4	Organizacija mora imeti podporno komunikacijsko in strojno opremo nameščeno v pogojih, ki so predpisani v specifikacijah uporabljene opreme.
Sklic:	
ETZ 4.2.1.5	Organizacija mora zagotoviti tehnično in uporabniško dokumentacijo za strojno opremo v uporabi.
Sklic:	

Dodatne zahteve za ponudnike storitev, ki jih ponujajo javnopravnim osebam

ETZ 4.2.1.6	*Ponudniki storitev, povezanih z zajemom in e-hrambo,* če jih ponujajo javnopravnim osebam, morajo za izvajanje teh storitev uporabljati pri državnem arhivu akreditirano strojno opremo.
Sklic:	

4.3 NOSILCI ZAPISA

ETZ 4.3.1.1	Organizacija mora z NP opredeliti nosilce zapisa, ki jih uporablja za dolgoročno e-hrambo.
Sklic:	
ETZ 4.3.1.2	Nosilec zapisa mora temeljiti na mednarodnih uveljavljenih in splošno sprejetih standardih, ki so široko priznani oz. uveljavljeni, njihova uporaba pa je podprta s strojno in programsko opremo, uveljavljeno na trgu.
Sklic:	
ETZ 4.3.1.3	Organizacija mora zagotoviti, da so vsi nosilci zapisa shranjeni in se uporabljajo oz. se z njimi ravna v stabilnem okolju.
Sklic:	
ETZ 4.3.1.4	Občasno, najmanj pa enkrat na leto je treba preverjati kakovost zapisa (uporabnost) na nosilcih in jih po potrebi menjati še pred pričakovanim potekom dobe trajanja.
Sklic:	

4.4 PROGRAMSKA OPREMA

4.4.1 Funkcionalni tipi programske opreme

ETZ 4.4.1.1 Programska oprema mora biti razvrščena v posamezen funkcionalni tip glede na raven uporabe, odnos med ponudnikom in stranko ter funkcionalnost.

Sklic:	

4.4.2 Zahteve za programsko opremo

ETZ 4.4.2.1 Programska oprema mora biti široko priznana in uveljavljena oz. uporabljana ali posebej razvita skladno z ZVDAGA, UVDAG in ETZ.

Sklic:	

ETZ 4.4.2.2 Programska oprema mora biti skladna z mednarodnimi, državnimi in drugimi splošno priznanimi standardi s področja zajema, e-hrambe in informacijske varnosti.

Opomba: Zahteva mora biti opredeljena z NP, ni pa predmet presoje NP temveč samo predmet preverjanja izvajanja NP.

Sklic:	

ETZ 4.4.2.3 Organizacija mora v NP navesti vsaj te podatke o programski opremi:

- identifikacijsko oznako oz. ime,
- komercialno oznako različice produkta,
- vse dodatne komponente vključno z različicami, ki sestavljajo programsko opremo in predstavljajo njeno določeno funkcionalnost.

Opomba: Glej tudi ETZ 3.1.1.1.

Sklic:	

Dodatne zahteve za ponudnike storitev, ki jih ponujajo javnopravnim osebam

ETZ 4.4.2.4 *Ponudniki storitev, povezanih z zajemom in e-hrambo,* če jih ponujajo javnopravnim osebam, morajo za izvajanje teh storitev uporabljati pri državnem arhivu akreditirano programsko opremo.

Sklic:	

4.4.3 Razvoj oz. nabava

ETZ 4.4.3.1 Organizacija mora imeti sprejeto dokumentirano metodologijo razvoja programske opreme oz. postopek njene nabave.

Sklic:	

ETZ 4.4.3.2	Poleg funkcionalnih zahtev programske opreme morajo biti opredeljene zahteve glede varovanja podatkov in skladnosti s predpisi.
Sklic:	
ETZ 4.4.3.3	Programska oprema mora biti pred uporabo preverjena oz. preizkušena (testirana) na podlagi dokumentiranega postopka, pri čemer se morajo poleg funkcionalnosti preveriti varnostni elementi in obremenitve.
Sklic:	
ETZ 4.4.3.4	Če organizacija pri razvoju in preizkušanju uporablja podatke iz produkcijskega okolja (okolje za redno rabo), mora glede zaupnosti ravnati z njimi enako skrbno, kakor se ravna z njimi v tem okolju. Po uporabi je treba testne podatke ustrezno uničiti.
Sklic:	
ETZ 4.4.3.5	Organizacija mora zagotoviti tehnično in uporabniško dokumentacijo za vso programsko opremo v uporabi.
Sklic:	

5 UPRAVLJANJE INFORMACIJSKE OPREME IN INFRASTRUKTURE

5.1 UPRAVLJANJE SPREMEMB

ETZ 5.1.1.1	Organizacija mora imeti formalno opredeljen in dokumentiran postopek upravljanja sprememb, ki zagotavlja, da so vse spremembe (npr. nadgradnja, vzdrževanje) na obstoječi informacijski opremi in infrastrukturi izvedene nadzorovano in pred uporabo preverjene. Postopek upravljanja sprememb mora vključevati najmanj: zahtevek za spremembo, analizo vplivov, odobritev, preizkušanje in uvedbo.
Sklic:	

5.2 LOČEVANJE OPERATIVNEGA OKOLJA OD OKOLJA, NAMENJENEGA RAZVOJU, IN OD OKOLJA ZA PREIZKUŠANJE

ETZ 5.2.1.1	Zagotovljeno mora biti ločevanje operativnega okolja od okolja, namenjenega razvoju, in od okolja za preizkušanje (testiranje).
Sklic:	

5.3 LOČEVANJE HRANJENEGA GRADIVA POSAMEZNIH ORGANIZACIJ

ETZ 5.3.1.1 *Ponudnik storitev* mora zagotoviti ustrezne ukrepe za ločevanje gradiva posameznih organizacij, za katere izvaja zajem in e-hrambo.

Sklic:	

5.4 ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO IN VDORI

ETZ 5.4.1.1 Vzpostavljena morajo biti pravila zaščite pred zlonamerno programsko opremo in vdori, ki vključujejo postopke za:

- zaščito strežnikov in delovnih postaj,
- nameščanje in posodabljanje programske opreme za zaščito,
- preverjanje delovanja zaščite,
- ukrepanje pri morebitni okužbi.

Sklic:	

5.5 SINHRONIZACIJA SISTEMSKIH UR

ETZ 5.5.1.1 Zagotovljen in opisan mora biti način uskladitve sistemskih ur (sinhronizacija) na strežnikih in ključnih delovnih postajah, če na njih teče kakšen servis, ki je del sistema za zajem in e-hrambo.

Sklic:	

5.6 VZDRŽEVANJE INFORMACIJSKE OPREME IN INFRASTRUKTURE

ETZ 5.6.1.1 Zagotovljena mora biti podpora in vzdrževanje za informacijsko opremo (strojno, programsko) ter infrastrukturo za zajem in e-hrambo s primernim odzivnim časom. Določene morajo biti odgovorne osebe za izvajanje rednega vzdrževanja. Vsi vzdrževalni posegi morajo biti dokumentirani.

Sklic:	

5.7 NADZOR, VARNOSTNI PREGLEDI IN ZAGOTAVLJANJE ZAPISOV O DELOVANJU SISTEMA

ETZ 5.7.1.1 Organizacija mora določiti postopke rednega spremljanja delovanja informacijskega sistema za zajem in e-hrambo v skladu z zahtevami zakona, ki ureja to področje, in internimi predpisi.

Sklic:	

ETZ 5.7.1.2 Zapisi o delovanju sistema se morajo hraniti najmanj do pregleda, ki ga izvede pooblaščena oseba in na podlagi katerega je pripravljen nov zapis o opravljenem pregledu in ustreznosti sistema.

Sklic:	

ETZ 5.7.1.3 Organizacija mora imeti vzpostavljen in dokumentiran notranji nadzor nad izvajanjem ukrepov za zagotavljanje informacijske varnosti, ki mora vključevati najmanj:

- načrt periodičnega izvajanja (časovna dinamika, način izvedbe),
- odgovorno osebo za področje, ki:
  - izdela poročilo o notranjem nadzoru z ugotovitvami glede pomanjkljivosti in s predlogi ukrepov za njihovo odpravo oz. zmanjšanje,
  - predstavi poročilo vodstvu.

Vodstvo določi način ter odgovorne osebe za izvedbo in spremljanje izvedenih ukrepov.

Sklic:	

Dodatne zahteve za ponudnike storitev e-hrambe:

ETZ 5.7.1.4 Ponudnik storitev e-hrambe mora opravljati redne varnostne preglede svoje informacijske infrastrukture vsak delovni dan. Rok hrambe poročil je najmanj do pregleda, ki ga izvede pooblaščena oseba in na podlagi katerega je pripravljen nov zapis o opravljenem pregledu in ustreznosti sistema.

Opomba: Če ponudnik zagotavlja storitve 24 ur na dan 365 dni na leto, mora varnostne preglede opravljati vsak dan.

Sklic:	

6 NAROČANJE STORITEV

6.1 POGODBENO UREJANJE IZVAJANJA STORITVE (MED NAROČNIKOM IN IZVAJALCEM)

ETZ 6.1.1.1 *Ponudnik in naročnik storitve* morata pred njenim opravljanjem poskrbeti za pripravo skupne ocene tveganja za posamezno storitev kot pisnega dokumenta, ki mora vsebovati najmanj:

- vrste in stopnjo tveganja pri zagotavljanju posamezne storitve,
- opis ukrepov glede na vrsto in stopnjo tveganja,
- porazdelitev odgovornosti med ponudnikom in naročnikom glede na oceno tveganja.

Opomba: Zahteva po pripravi skupne ocene tveganja mora biti vključena v določbe NP , ni pa v NP treba vključevati skupnih ocen tveganja. Skupne ocene tveganja so predmet preverjanja izvajanja NP.

Sklic:	

ETZ 6.1.1.2	Naročanje storitev pri zunanjem izvajalcu mora biti pogodbeno urejeno v skladu z zakonodajo, natančno določenim obsegom storitve in ravnjo opravljanja storitve in ugotovitvami skupne ocene tveganj. V pogodbi morajo biti opredeljeni: ▪ natančen obseg storitve, ▪ raven storitve − kakovostna in časovna opredelitev (spremljajoča dokumentacija, odzivni časi, dostopnost …), ▪ odgovornost naročnika in zunanjega izvajalca pri izvajanju posameznih postopkov v skladu z obsegom storitve, ▪ način varovanja podatkov in podpis izjave o zaupnosti oz. varovanju informacij, ▪ pravica naročnika do rednega pregleda opravljanja storitve zunanjega izvajalca, pri čemer se preverijo predvsem: splošna organizacija in notranja pravila, upravljanje informacijskega sistema, varnostno področje, upravljanje dokumentacije.
Sklic:	*Opomba: Zahteva ne velja za ponudnike storitev.*

6.2 IZVAJANJE STORITEV ZA JAVNOPRAVNE OSEBE

ETZ 6.2.1.1	Storitve zajema in e-hrambe arhivskega gradiva oz. s tem povezane spremljevalne storitve sme za javnopravne osebe opravljati samo ponudnik, ki je te storitve akreditiral pri državnem arhivu.
Sklic:	

II. OBRAZLOŽITEV IN DODATNA POJASNILA

1. NOTRANJA PRAVILA IN ORGANIZACIJA

1.1. SPLOŠNO O NOTRANJIH PRAVILIH (NP)

Po ZVDAGA so NP interni pravni akt, s katerim organizacija ureja zajem in e-hrambo gradiva, ponudniki pa opravljanje storitev.[3] Dokazljivo opravljanje dejavnosti v skladu z NP, ki so usklajena z zahtevami ZVDAGA in podrejenimi predpisi, zagotavlja priznanje avtentičnosti gradiva, ki se obravnava.[4] Skladnost NP s predpisi ugotavlja državni arhiv v posebnem postopku potrjevanja. Z NP med drugim določimo:

- poslovne funkcije,
- delovne postopke, ki jih bodo zaposleni v organizaciji izvajali za zagotovitev ustreznega in učinkovitega zajema in e-hrambe gradiva oz. spremljevalnih storitev,
- delovna mesta, ki so vključena v opravljanje posameznih dejavnosti pri zajemu in e-hrambi oz. spremljevalnih storitev.

Namesto lastnih NP lahko organizacija prevzame **vzorčna notranja pravila** druge organizacije, če jih je ta pripravila za širšo uporabo. Ta pravila so primerna za tiste, ki poslujejo enako ali zelo podobno, saj jih je treba prevzeti v celoti in brez sprememb. V tem primeru ni treba, da Arhiv RS ponovno potrjuje NP.

1.1.1 Predhodna priprava na zajem in e-hrambo

Predpisi določajo, da se NP pripravijo na podlagi predhodne priprave na zajem in e-hrambo, ki mora biti dokumentirana v poročilu. Poročilo o predhodni pripravi se mora priložiti vlogi za potrditev NP in mora vključevati najmanj:

- analizo obstoječega stanja,
- zahteve za e-hrambo,
- študijo izvedljivosti e-hrambe,
- načrt e-hrambe.

Analiza obstoječega stanja:

Izvedemo jo na podlagi:

- pregleda dejavnosti organizacije,
- popisa poslovnih in pravnih zahtev (zakonodaja, ki jo mora organizacija upoštevati pri zajemu in e-hrambi oz. s tem povezanih storitvah),
- popisa vrst in virov gradiva, ki nastaja oz. bo zajeto in e-hranjeno.

Pregled dejavnosti organizacije:
Organizacijo pregledamo z vidika:

- njenega poslanstva in njene pristojnosti,
- veljavne zakonodaje, ki je pomembna za upravljanje gradiva in njegovo hrambo,
- postopkov, ki izhajajo iz temeljnih poslovnih funkcij organizacije (npr. nabava, prodaja, kadrovski, finančni in upravljavski postopki), vključenih v sistem zajema in e-hrambe,

[3] ZVDAGA, 2. in 18. člen.

[4] ZVDAGA, 32. člen.

- notranje organizacije, npr. vloga, veščine[5] in usposobljenost zaposlenih v okviru evidentiranih poslovnih funkcij, njihova vključenost v postopke zajema in e-hrambe, ter to primerjamo s potrebami in zahtevami sistema e-hrambe gradiva,
- obstoječih predpisov (npr. pravilniki, navodila) v organizaciji in širše, ki so povezani z evidentiranimi poslovnimi funkcijami,
- itd.

Popis vrst in virov gradiva

Popišemo vrste in vire gradiva, ki nastaja pri evidentiranih poslovnih funkcijah. Tako npr.:
- v *poslovni funkciji upravljanja zaposlenih* (kadrovska služba) nastaja gradivo, kakršne so osebne mape in pripadajoča dokumentacija, druge kadrovske evidence, kadrovski načrti, pogodbe o zaposlitvi, podjemne in avtorske pogodbe;
- v *poslovni funkciji nabave* nastaja gradivo, kakršne so naročilnice, dobavnice, evidence zalog, vhodni računi, reklamacije, uporabniška navodila in specifikacije;
- v *finančnih poslovnih funkcijah* nastaja gradivo, kakršni so zaključni računi, bilance, finančni načrti, finančne analize, poslovne knjige, knjigovodske listine in obračuni plač.

Ko popisujemo gradivo in njegove vire, moramo upoštevati, da pri poslovanju organizacije nastaja gradivo, ki se razlikuje po vsebini, nosilcu in formatu zapisa (npr. slike, preglednice, filmi, magnetogrami) ter po zahtevah glede upravljanja in rokov hrambe. Lahko nastaja tudi gradivo, ki mora biti še posebej varovano, ker vsebuje osebne podatke, za katere veljajo stroga določila Zakona o varstvu osebnih podatkov, ali različne vrste zaupnih podatkov (poslovna skrivnost, bančna in davčna tajnost, podatki s stopnjo tajnosti v javni upravi). Del gradiva, ki nastaja pri poslovanju, je lahko tudi arhivsko gradivo.

Zahteve za e-hrambo:

Zahteve za e-hrambo opredelimo kot pravne, tehnološke in poslovne. Predpisane so predvsem v ZVDAGA, UVDAG, ETZ in področni zakonodaji (npr. glede rokov hrambe). Poslovne zahteve se npr. nanašajo na razpoložljivost, varnost in zanesljivost sistema e-hrambe (opreme, storitev, gradiva) ter na skladnost s predpisi.

Pri določitvi zahtev za e-hrambo upoštevamo:
- obliko, vsebino, občutljivost in roke hrambe gradiva, med drugim:
  - katere vrste gradiva imamo in v kakšnih formatih ga bomo hranili,
  - katere metapodatke imamo in kako jih bomo hranili,
  - ali je gradivo elektronsko podpisano oz. časovno žigosano,
  - ali je gradivo zaupne narave,
  - ali je del gradiva tudi arhivsko gradivo;
- zahtevano oz. pričakovano razpoložljivost informacijskega sistema (npr. v kolikšnem času mora biti gradivo dostopno ob morebitni katastrofi);
- politiko dostopov do gradiva (npr. pravila dodeljevanja/odvzemanja dostopov do informacijskih virov);
- zahtevano varnost pri prenosu gradiva (npr. ali obstajajo zakonske ali druge poslovne zahteve za zagotavljanje varnosti pri prenosu gradiva po komunikacijskih kanalih);
- potrebe po sledljivosti vseh sprememb v sistemu e-hrambe itd.

Študija izvedljivosti e-hrambe

[5] Zahtevane veščine so opredeljene npr. z opisi delovnih mest, pogodbami o zaposlitvi.

S to študijo podrobneje proučimo izvedljivost e-hrambe in ugotovimo, kakšna je njena najboljša možna izvedba, ki bo skladna z zakonskimi določili (ZVDAGA, UVDAG, ETZ), pa tudi priporočili standardov (npr. ISO 14721:2003 (OAIS)), tehnološkimi trendi ter dobrimi praksami upravljanja dokumentov in arhivske stroke po svetu.

Pri izdelavi študije izvedljivosti upoštevajmo:

- ali obstajajo in katere so poslovne potrebe za izvedbo e-hrambe (npr. zakonske, pogodbene),
- ali imamo vse potrebne vire za izvedbo e-hrambe (npr. kadrovske, finančne),
- ali e-hrambo v danem okolju lahko vzpostavimo (npr. so naše poslovne funkcije elektronsko podprte, imamo ustrezno infrastrukturo).

Načrt e-hrambe:

Načrt e-hrambe je akcijski načrt za organizacijo, vzpostavitev sistema za zajem in e-hrambo ter potreben informacijski sistem. V njem predvidimo najmanj:

- način izvedbe (poslovni model),
- poslovne funkcije, ki bodo predmet zajema in e-hrambe, ter odgovornost za njihovo izvajanje,
- uporabniške, poslovne in tehnološke zahteve za informacijski sistem za zajem in e-hrambo,
- načrt usposabljanja,
- načrt organizacijskega in tehnološkega vzdrževanja,
- načrt prehoda na novo organizacijo in nov informacijski sistem (po potrebi) ter s tem povezane morebitne pretvorbe gradiva iz ene oblike v drugo.

1.1.2 Notranja pravila za zajem in e-hrambo

NP morajo biti odsev zakonskih zahtev, notranje organizacije in uporabljene tehnologije. Njihovo okvirno vsebino določa UVDAG[6], upoštevati pa je treba tudi določbe, ki izhajajo neposredno iz ZVDAGA in teh ETZ. Predpisi določajo, da morajo javnopravne osebe in ponudniki storitev zajema in e-hrambe ter spremljevalnih storitev svoja notranja pravila obvezno dati v potrditev državnemu arhivu.

1.1.3 Nadzor nad izvajanjem NP

Redno spremljanje delovanja v skladu z NP zagotavlja odkrivanje morebitnih pomanjkljivosti in napak. Samo formalno zapisana NP niso zadosten pogoj za priznavanje pravne veljavnosti in dokazne vrednosti gradiva v digitalni obliki že na podlagi zakona. Organizacija jih mora tudi dokazljivo izvajati. Pri preverjanju se presoja skladnost izvajanja NP, kar vključuje tudi stalno preverjanje delovanja informacijskega sistema za e-hrambo in drugih s tem povezanih sistemov.

Zakonsko predpisano je obvezno preverjanje (spremljanje) izvajanja NP, in sicer kot notranje in zunanje preverjanje. Izvaja se na podlagi zakonskih zahtev in NP, ki jih je potrdil državni arhiv. O preverjanjih (notranjih in zunanjih) mora obstajati poročilo z vsemi ugotovitvami o izpolnjevanju ali odmiku delovanja od NP. Poročilo mora vsebovati najmanj te podatke:

- datum in kraj izvedbe preverjanja,
- odgovorne osebe (presojevalci),
- namen preverjanja (načrtovana, ponovna ali izredna presoja),
- katera področja NP so bila preverjena (naslov dokumenta, različica),

[6] UVDAG, 5. člen.

- ugotovitve, odmiki od izvajanja NP, dokazila, predlog priporočil oz. ukrepov za odpravo odmikov, tip ukrepa (preventivni, kurativni), rok izvedbe ukrepa, odgovorne osebe za izvedbo ukrepa.

Notranje preverjanje

Notranje preverjanje je obvezno za vsako organizacijo z NP, ki jih potrdi državni arhiv. V skladu z načrtom presoje izvajanja NP to preverjanje vsaki dve leti[7] opravi posameznik ali skupina presojevalcev, ki jih določi poslovodni organ.

Zunanje preverjanje

Zunanje preverjanje se opravi pri storitvah zajema oz. e-hrambe pomembnega gradiva oz. s tem povezanih spremljevalnih storitvah (sem vsekakor spada arhivsko gradivo). Opravi se tudi ob akreditaciji vseh teh storitev (pri njihovih ponudnikih).

Zunanje preverjanje izvajanja NP ***pri javnopravnih osebah*:**

- Poteka po načrtu presoje izvajanja NP ali po strokovnem navodilu pristojnega arhiva, s katerim se določijo obseg in pogoji tega preverjanja.
- Opravijo ga preizkušeni revizorji informacijskih sistemov[8], in sicer enkrat na leto ali na podlagi odločitve pristojnega arhiva.

Zunanje preverjanje izvajanja NP ***pri ponudnikih storitev zajema in e-hrambe gradiva ter spremljevalnih storitev*:**

- Poteka v skladu z načrtom presoje izvajanja NP.
- Opravi se ob vložitvi zahtevka za akreditacijo storitve zajema in e-hrambe oz. spremljevalnih storitev.
- Opravi se ob podaljšanju že podeljene akreditacije storitve zajema in e-hrambe oz. spremljevalnih storitev.
- Opravi se redno enkrat na leto, lahko pa tudi izredno.
- Opravijo ga preizkušeni revizorji informacijskih sistemov, pri akreditaciji storitve pa državni arhiv v sodelovanju s preizkušenimi revizorji informacijskih sistemov.

1.2. NOTRANJA ORGANIZACIJA, VLOGE IN USPOSOBLJENOST OSEBJA

1.2.1 Notranja organizacija

Za opravila, ki so pomembna za ustrezno izvedbo zajema oz. e-hrambe, morajo biti določene odgovorne osebe. Za vsako delovno mesto, povezano z zajemom oz. e-hrambo, morajo biti poleg splošnih zahtev določeni opis nalog in morebitni varnostni pogoji. Med splošne zahteve spadajo zahteve o izobrazbi, strokovni usposobljenosti, delovnih izkušnjah ipd. Navadno se te zahteve določijo v aktu o sistemizaciji delovnih mest v organizaciji.

Če akt o sistemizaciji delovnih mest med pogoji za sklenitev pogodbe o zaposlitvi oz. za zasedbo delovnega mesta določa tudi varnostne pogoje, ki jih mora za zaposlitev oz. zasedbo delovnega mesta izpolnjevati posameznik, morajo ti pogoji temeljiti neposredno na veljavnih zakonskih podlagah (npr. pogoji, ki jih za obravnavanje tajnih podatkov zahteva Zakon o tajnih podatkih in

[7] UVDAG, sedmi odstavek 9. člena.

[8] Preizkušeni revizor informacijskih sistemov je strokovnjak z raznovrstnim specialističnim znanjem o uporabi informacijske tehnologije, ki je po opravljenem izpitu CISA (Certified Information System Auditor, **CISA)** pri Slovenskem inštitutu za revizijo pridobil naziv preizkušeni revizor informacijskih sistemov.

predpisi, izdani na njegovi podlagi; pogoji, ki jih za imenovanje v naziv določa Zakon o javnih uslužbencih) in na oceni tveganja.

Organizacija mora zagotavljati:

- urejenost (postavljena pravila za izvajanje delovnih postopkov),
- usposobljenost zaposlenih za delo z informacijsko infrastrukturo,
- zavedanje vseh zaposlenih o pomenu varovanja informacij in dosledno upoštevanje varnostnih pravil,
- kakovostno podporo informacijske infrastrukture (skrbna in strokovna izbira programske in strojne opreme, uvajanje in vzdrževanje v skladu z dobrimi praksami in pravili stroke),
- reden nadzor nad izpolnjevanjem zgornjih zahtev in določitev odgovornih oseb za ta nadzor.

1.2.2 Usposobljenost zaposlenih, ki delajo z gradivom v digitalni obliki

Ustrezno ravnanje z gradivom v digitalni obliki temelji na odgovornih in ustrezno usposobljenih zaposlenih, ki morajo imeti poleg splošne izobrazbe še ustrezno strokovno znanje oz. usposobljenost. Organizacija mora v postopku nove zaposlitve ali notranje prerazporeditve zaposlenega na delovno mesto, povezano z zajemom oz. e-hrambo, preveriti, ali kandidat izpolnjuje vse varnostne in druge pogoje, predpisane za to delovno mesto. Varnostni zadržek je lahko npr. dostop do tajnega gradiva po Zakonu o tajnih podatkih, če zaposleni nima ustreznega dovoljenja za ta dostop. Po tem zakonu mora namreč imeti dovoljenje za dostop do tajnih podatkov, ki ga pridobi na podlagi varnostnega preverjanja. Varnostno preverjanje osebe je poizvedba, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ, da pridobi vse potrebne podatke o morebitnih varnostnih zadržkih.

Organizacija se mora prepričati, ali ne obstajajo zakoniti varnostni zadržki glede uporabe informacijskih virov, ki jih bo zaposleni uporabljal pri svojem delu.

Dodatni pogoji za zaposlene pri javnopravni osebi in ponudniku storitev

Za zaposlene pri javnopravni osebi ali ponudniku storitev veljajo še dodatni pogoji, ki jih določa ZVDAGA[9] in na njegovi podlagi sprejeti podzakonski akti[10].

2. ZAJEM IN E-HRAMBA TER SPREMLJEVALNE STORITVE

2.1. SPLOŠNO O DELOVNIH POSTOPKIH

Z NP morajo biti opredeljeni delovni postopki ali njihovi deli, ki vplivajo na celovitost in verodostojnost obravnavanega gradiva v digitalni obliki, npr.:

- zajem gradiva v fizični obliki v ISUD (digitalizacija),
- zajem gradiva v digitalni obliki v ISUD (uvoz zapisov ali (meta)podatkov v ISUD, ročni vnosi (meta)podatkov v ISUD),
- pretvorba gradiva iz ene v drugo digitalno obliko,
- hramba gradiva v digitalni obliki,
- urejanje in/ali popisovanje gradiva,
- odbiranje arhivskega gradiva iz dokumentarnega gradiva,

[9] ZVDAGA, 39. člen, 89. člen.
[10] UVDAG, 21. člen; Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom (Uradni list RS, št. 132/06 in 38/08).

- izločanje in uničevanje dokumentarnega gradiva.

Organizacija mora zagotoviti ustrezen način dela tako, da so jasno določene odgovornosti za opravila, pomembna za ustrezno izvedbo zajema in e-hrambe oz. izvajanje NP.

Za vsak izvajani delovni postopek določimo:

- *njegov namen;*

  z namenom opredelimo učinke, ki jih bomo dosegli z izvedbo delovnega postopka (npr. zajem digitalizacija dokumentarnega gradiva, pretvorba gradiva v obliko za dolgoročno hrambo, uničevanje gradiva, ki mu je potekel rok hrambe, odbiranje arhivskega gradiva iz dokumentarnega v skladu z navodili pristojnega arhiv);

- *naročnika postopka*;

  naročnik postopka je tista oseba, ki določa zahteve za izdelke rezultate postopka ter merila za njihovo ustreznost slednjih (npr. zaposleni v organizaciji, ki bodo uporabljali dokumente digitalizirane v tajništvu, naročnik storitve hrambe, ki bo dostopal do gradiva hranjenega pri ponudniku storitve);

- *odgovorne osebe*;

  odgovorna oseba je tista oseba, ki je zadolžena za opredelitev postopka, kar pomeni, da v skladu z zahtevami naročnika določi način izvajanja postopka, nadzorovanje njegovega izvajanja in preverjanje uspešnosti izvedbe. Odgovorna oseba je običajno neposredno nadrejena izvajalcem postopka. V primeru, ko se postopek (npr. sprotna digitalizacija) izvaja v več organizacijskih enotah, je lahko odgovornih oseb več (za vsako organizacijsko enoto). V primeru, ko postopek poteka v okviru izvajanja storitve, za katero je najet zunanji ponudnik, je primerno, da določita tako naročnik kot ponudnik vsak svojo odgovorno osebo;

- *vhode v postopek;*

  vhodi so vsi tisti zapisi, podatki ali informacije, ki so nujno potrebni za izvedbo postopka. V postopkih zajema in hrambe gradiva so najpogostejše oblike vhodov: najprej gradivo samo, nato metapodatki, ki opisujejo posamezno enoto gradiva (lahko so zapisani v gradivu in je zgolj pojasnjeno kako jih izvajalec identificira, lahko pa so gradivo dodani v posebnih zapisih), zahteve naročnika, ki natančneje opisujejo pričakovane rezultate, informacije o posebnih zahtevah pri izvajanju postopka (npr. fizična občutljivost gradiva, vsebovanost občutljivih podatkov). Če so predmet obdelave v postopku zapisi z različnimi lastnostmi (npr. različni tipi gradiva: računi, tehnična dokumentacija, spisovno gradivo), so pogosto tudi vhodi v postopek specifični za vsako skupino zapisov (npr. podatki, zapisi, dokumenti kot predmet obdelave). Če so izdelki postopka določeni z različnimi zahtevami (npr. različna ločljivost digitalizirane slike), tudi ti spadajo k vhodu;

- *izhode iz postopka;*

  izhodi, to so vsi rezultati izvajanja procesa. Med njimi so na prvem mestu izdelki, ki jih potrebujejo naročniki, med njimi pa je vedno tudi vsa dokumentacija, ki je nastala pri izvajanju postopka;

- *način preverjanja uspešnosti izvedbe postopka;*

  za vsak delovni postopek je ključno, da ob njegovem oblikovanju določimo merila, ki opredeljujejo zahtevano kakovost izdelka, rezultate postopka ter njihovo pravočasnost. Ob tem je treba določiti tudi način in obseg preverjanja. Pristojnost določanja meril za

ugotavljanje uspešnosti izvedbe postopka ima naročnik. Opis preverjanja uspešnosti izvedbe postopka mora vključevati tudi opravila za odpravo odkritih napak.

2.2. PRIPRAVA NA ZAJEM

2.2.1 Evidentiranje gradiva

Ureditve sprejemanja in odprave gradiva ne določajo ZVDAGA, UVDAG in ETZ, temveč predpisi o upravljanju dokumentarnega gradiva. Pri urejenem upravljanju se vsi dokumenti razvrstijo, označijo in evidentirajo že ob svojem nastanku, odprava pa je le sestavni del evidence. ETZ določajo le, da morajo biti dokumenti, ki jih nameravamo zajeti oz. pretvoriti, evidentirani, kar pomeni, da morajo biti uvrščeni v ISUD.

Z evidentiranjem gradivo formalno uvrstimo v sestav dokumentarnega gradiva organizacije (pri elektronskem upravljanju gradiva v ISUD). Pri tem nastaja evidenca, ki je lahko v fizični (knjiga, kartoteka) ali elektronski obliki. Evidenco o gradivu v elektronski obliki lahko oblikujemo ročno ali pa jo ISUD oblikuje samodejno.

Namen evidence je, da:

- dokazuje obstoj gradiva oz. dejanje, ki ga gradivo izraža, opisuje, riše, prikazuje,
- zagotavlja osnovne podatke o gradivu (kdo ga je ustvaril, kdaj je nastalo, o čem govori itd.),
- pokaže mesto dokumenta (gradiva) v organizacijski sestavi organizacije,
- omogoča iskanje gradiva v nekem sestavu (organizaciji).

2.2.2 Razvrščanje (klasificiranje) gradiva

Gradivo lahko razvrščamo po njegovi vsebini, vrstah in oblikah ali uporabimo kombinacijo teh načinov. Podlaga za to je načrt razvrščanja gradiva (klasifikacijski načrt).

Postopek razvrščanja mora biti v notranjih pravilih opredeljen na način, da bodo jasni odgovori na naslednja vprašanja:

- Kdo (katera delovna mesta) razvršča gradivo in kdo so odgovorne osebe (katera delovna mesta), ki skrbijo, da razvrščanje poteka v skladu z notranjimi pravili?

  (V večjih organizacijah lahko poteka razvrščanje v okviru organizacijskih enot, v manjših pa je običajno, da se razvršča na enem mestu npr. v tajništvu, glavni pisarni organizacije.)

- Kdaj se gradivo razvršča?

  (Običajno poteka razvrščanje v okviru procesa evidentiranja gradiva, najkasneje pa mora biti gradivo razvrščeno ob njegovi uvrstitvi s stalno zbirko.)

- Kaj je podlaga za razvrščanje gradiva?

  (V notranjih pravilih mora biti jasno določeno, kaj je vsebina načrta razvrščanja in kaj so njegovi elementi: znak, opis vsebine znaka, rok hrambe. Če se za različne skupine gradiva uporabljajo različni načini razvrščanja, je treba v notranjih pravilih jasno določiti, za katere skupine gradiva velja kateri načrt razvrščanja.)

Pri opisu oz. opredelitvi postopka razvrščanja je treba smiselno uporabljati določila iz ETZ 2.1.1.1.

Oseba, ki je odgovorna za skrbništvo nad načrtom razvrščanja mora skrbeti, da je zaposlenim vedno dostopna veljavna različica načrta. Pri spremembah načrta, pa mora poskrbeti, da so spremembe jasno vidne in da se trajno hranijo starejše različice načrtov.

2.2.3 Dodeljevanje gradiva v reševanje oz. dodeljevanje pravic, nalog in odgovornosti (signiranje)

S postopkom dodeljevanja gradiva v reševanje in s tem povezanih pravic, nalog in odgovornosti omogočimo dostop in ustrezna pooblastila pri uporabi dokumentarnega gradiva (branje, spreminjanje, brisanje itd.).

Določena morajo biti delovna mesta, odgovorna za izvedbo posameznih nalog, in ne posamezniki, ki jih zasedajo. Načrt znakov sestavi organizacija sama na podlagi akta o notranji organizaciji in sistematizaciji delovnih mest.

V *večjih* organizacijah ima vsaka organizacijska enota svoj znak, delovna mesta v teh enotah pa podznak (na primer: oddelek za okolje in prostor 10, vodja oddelka 110, svetovalec za stanovanjske zadeve 111, svetovalec za gradbene zadeve 112 itd.).

V *majhnih* organizacijah brez organizacijskih enot pa dobi vsako delovno mesto svoj znak (na primer: direktor 1, komercialist 2, računovodja 3 itd.). Znak je lahko številčen, črkoven ali kombinacija obeh.

2.2.4 Roki hrambe

Rok hrambe je čas hrambe gradiva. Glede na to ločimo:

- arhivsko gradivo, ki ima trajen pomen za znanost in kulturo ali pravno varnost države, njenih institucij in posameznikov,
- trajno gradivo, ki ima trajen pomen za organizacijo, pri kateri je nastalo, ali pa ga je treba trajno hraniti, ker tako določajo zakonski predpisi,
- gradivo z omejenim rokom hrambe (2, 3, 5, 10 let ali več), ki nima narave arhivskega gradiva niti ga ni treba trajno hraniti iz poslovnih ali drugih razlogov.

Rok hrambe mora biti naveden (določen) v načrtu razvrščanja gradiva organizacije (klasifikacijskem načrtu).

2.3. ZAJEM GRADIVA

Elektronski zapisi izhajajo iz notranjih in zunanjih virov. Vključevanje (zajemanje) v informacijski sistem je lahko različno. Med postopkom je treba prepoznati vse morebitne potrebe po pretvorbi in hrambi v različnih oblikah zapisa (formata), pa tudi druge posebnosti ob evidentiranju in sledenju. Pojem »zajem« vključuje tudi postopke evidentiranja dokumenta, uvrstitev v ustrezno skupino po načrtu razvrščanja in dodajanje metapodatkov.

Pri zajemu gradiva je treba poskrbeti, da se pretvori pravilno. Če naj bo njegova hramba enakovredna hrambi izvirnega gradiva, mora zajeto gradivo zagotavljati in ohranjevati vse učinke izvirnega gradiva[11].

Standardi in priporočila, ki urejajo posamezno vrsto gradiva, so navedeni v prvem delu ETZ: Uvodna poglavja, IV. poglavje.

2.3.1 Zahteve za metapodatke

Če metapodatke razložimo dobesedno, so to »podatki o podatkih« ali natančneje, podatki o gradivu.[12] Sistemi za upravljanje in hrambo dokumentarnega gradiva v digitalni obliki morajo

[11] Temeljno načelo ohranjanja dokumentarnega gradiva oz. ohranjanja njegove vsebine je vsebovano v 3. členu ZVDAGA, po katerem je ta hramba *»ohranjanje izvirnega dokumentarnega gradiva ali uporabnosti vsebine tega gradiva«*.

podpirati širok spekter različnih metapodatkov. Ta je odvisen od vrste oz. tipa gradiva (npr. besedilni in mešani dokumenti, film in avdiovizualno gradivo, spletne strani, elektronska pošta, podatkovne zbirke in uradne evidence) ter od potreb in namenov posameznega sistema oz. upravljanega gradiva. Zaradi slednjega lahko vključujejo npr. tudi mesto v vnaprej določenem načrtu razvrščanja (klasifikacijski shemi), omejitve in beleženje dostopa do posameznih dokumentov, ključne besede, povezave z drugimi dokumenti itd.

Metapodatki se lahko zapisujejo in hranijo ločeno od samega zapisa ali v samem zapisu, kadar to omogoča njegova izbrana oblika in je na voljo orodje za njihov priklic. Pravilno uporabljeni omogočajo:

- priklic (iskanje in najdbo),
- podporo postopkom upravljanja dokumentov,
- prikazovanje povezav med dokumenti, ki skupaj tvorijo zaključeno vsebinsko enoto gradiva (zadeva, spis, dosje),
- dokazovanje izvora dokumentov (okoliščine, v katerih so nastali ali bili sprejeti),
- zagotavljanje celovitosti in avtentičnosti dokumenta,
- uporabnost (v povezavi s tehnološkimi platformami).

2.3.2 Oblika zapisa pri zajemu

Gradivo je lahko hranjeno v različnih oblikah zapisa. Te so odvisne od vrste gradiva, od njegove vsebine in načina uporabe. Najpogosteje govorimo o oblikah zapisa za:

- t. i. pisarniške zbirke (npr. oblikovano besedilo, razpredelnice, predstavitve),
- »golo« besedilo (z znaki izbrane kodne tabele),
- slikovno gradivo (rastrski, vektorski zapisi),
- avdiovizualno gradivo,
- podatkovne zbirke (vključujejo zgoraj naštete oblike zapisa, hkrati pa sestava zbirke zahteva dodatne posebnosti),
- spletno gradivo.

Posebne oblike zapisa so namenjene specifičnim vrstam gradiva ali pa so primerne za kombinacijo zgoraj omenjenih vrst. Pri večini oblik zapisa naredimo kompromis glede na kakovost, velikost in način uporabe digitalnega objekta. Znotraj vsake skupine ločimo:

- produkcijske oblike zapisa, ki so odvisne od izvornega orodja, s katerim je zapis nastal oz. se uporablja;
- oblike zapisa za kratkoročno in dolgoročno hrambo.

ZVDAGA vsebuje zgolj splošne določbe, po katerih je pri hrambi izvirnega ali zajetega gradiva v digitalni obliki treba zagotoviti dostopnost, uporabnost, celovitost in avtentičnost (26. in 27. člen).

Ko so dokumenti v ISUD še v aktivni fazi življenjskega cikla, lahko obliko zapisa določimo na dva načina:

- Prvi način določa, da se v trenutku nastanka ali čim prej po tem dokument že zapiše v obliki za dolgoročno hrambo, ki je vnaprej določena.

[12] Standard ISO 15489-1 definira metapodatke kot »podatke, ki opisujejo kontekst, vsebino in strukturo dokumentov (records) in njihovo upravljanje skozi čas.«

- Drugi način je, da se v kratkoročno hrambo sprejmejo vse oblike zapisa, ki nastanejo pri poslovanju ter so navadno oblikovane za kar najučinkovitejše upravljanje in poslovanje. Šele pri zajemu v dolgoročno hrambo dobijo ustrezne oblike za tako hrambo.

Produkcijske oblike zapisa so odvisne od posebnih programov in orodja, s katerimi je bilo gradivo ustvarjeno. Dodatne težave lahko nastanejo pri lastniških oblikah zapisa, katerih uporaba ni prosta in je pogosto odvisna od licenc, posebne opreme, razširjenosti ipd. Obstaja veliko različnih oblik zapisa, ki se sproti in pogosto nadgrajujejo ter niso združljive s starejšimi različicami programske opreme, namenjene prikazu in pretvorbi teh oblik. Zaradi vsega naštetega produkcijske oblike zapisa praviloma ne omogočajo zadovoljive rešitve za varno dolgoročno hrambo gradiva. Zato je velikega pomena zmožnost pretvorbe iz produkcijskih v druge oblike.

2.3.3 Besedilni in mešani dokumenti

V tej skupini so dokumenti, kakršne ustvarjamo npr. s sodobnimi t. i. »zbirkami pisarniških programov«, s katerimi urejamo besedila, razpredelnice, predstavitve. Če se namesto na tip osredotočimo na vsebino gradiva, gre najpogosteje za upravno-poslovno dokumentacijo v poslovnem okolju in spisovno gradivo, ki ga vodimo v evidenci dokumentarnega gradiva. Omenimo še specifične vrste gradiva, kakršne so finančna, računovodska in knjigovodska dokumentacija[13], projektna in tehnična dokumentacija[14], šolska dokumentacija[15], medicinska dokumentacija[16] itd.

V prizadevanju za usklajeno in učinkovito upravljanje *celotnega* dokumentarnega gradiva organizacije vključujemo tudi specifično gradivo v celoto dokumentarnega gradiva, organizirano z uporabo enega načrta za razvrščanje (klasifikacijskega načrta). Nekatere vrste specifičnega gradiva lahko uvrstimo v klasifikacijski načrt v zanje ustvarjene vsebinske razrede, druge s tem načrtom vsaj povežemo – posebni evidenci tega gradiva dodelimo znak ustreznega razreda v načrtu za razvrščanje (klasifikacijskem načrtu).

Po UUP[17] za specifično gradivo evidence o zadevah in dokumentih niso obvezne (ni jih treba nujno uvrstiti v zbirko dokumentarnega gradiva oz. evidentirati v njej), ampak za ravnanje z njim uredba predvideva določitev posebnih pravil na podlagi predpisov, smiselno upoštevajoč določila UUP o ravnanju z gradivom.

2.3.4 Film in avdiovizualno gradivo

V tem poglavju so navedene dodatne zahteve za to vrsto gradiva, omejene predvsem na obvezni izbor metapodatkov. Sicer pa za to gradivo veljajo enake zahteve kakor za drugo gradivo.

2.3.5 Spletne strani

Spletni dokument je dokument, ki je:

---

[13] Slovenski računovodski standardi (Uradni list RS, št. 118/2005).
Zakon o davku na dodano vrednost /ZDDV-UPB3/ (Uradni list RS, št. 25-874/2005).
Zakon o davčnem postopku /ZDavP-1-UPB1/ (Uradni list RS, št. 25-872/2005).

[14] Zakon o graditvi objektov /ZGO-1/ (Uradni list RS, št. 102/2004, 14/2005, 120/2006 in 126/07).
Pravilnik o projektni dokumentaciji (Uradni list RS, št. 55/2008).

[15] Npr. Pravilnik o dokumentaciji v devetletni osnovni šoli (Uradni list RS, št. 61/2005).

[16] Zakon o zbirkah podatkov s področja zdravstvenega varstva /ZZPPZ/ (Uradni list RS, št. 65/2000).

[17] UUP, 125. člen.

- objavljen za prenos po medmrežju (internet), je na voljo po spletnem vmesniku (navadno spletni brskalnik) in na spletnem mestu, ki se uporablja za objavo oz. pošiljanje vsebin ali za izvajanje storitev;
- lahko spletna stran, ki je na voljo za dostop po protokolu http (URL-naslov), ali drug dokument, obrazec, objekt, element, objavljen z uporabo identifikatorja URI[18].

Slovenska zakonodaja obravnava problematiko ustvarjanja, zajema in hrambe spletnih dokumentov. Javnopravne osebe so s pravnimi akti celo zavezane, da nekatere podatke objavljajo na spletu (npr. javna naročila, objava prostih delovnih mest). Za javni in za zasebni sektor pa velja ZVDAGA[19] s pripadajočimi podzakonskimi akti[20].

Organizacija, ki gradivo objavi na spletnem mestu, mora zaradi pravnih ali drugih zahtev take dokumente obravnavati enako kakor vse drugo dokumentarno gradivo. Spletni dokument je lahko sestavljen iz ene ali več komponent, ki so razporejene v neko celoto. Če je na spletu objavljen le kot kopija izvirnika, ki je v enaki obliki že na voljo v sistemu za upravljanje dokumentov, zanj zajem v okviru zajema spletne strani ni potreben, saj je že zajet in hranjen kot del dokumentarnega gradiva v ISUD. Vendar je treba v ISUD zapisati, da je bil dokument objavljen na spletni strani, URI take strani, datum in čas objave ter odgovorno osebo. Drugače je seveda z gradivom, ki je samo v spletni obliki ali prikazano iz zalednega informacijskega sistema s svojo podatkovno zbirko. V tem primeru so zahteve za hrambo odvisne od:

- načina razvrstitve gradiva,
- narave delovanja osebe in objavljanja spletnih dokumentov (stopnja odgovornosti glede objavljenih vsebin je npr. večja pri organizaciji, katere spletni dokumenti vplivajo na javnost),
- namena spletnega mesta (npr. objava informacij, komunikacija, storitve),
- kompleksnosti spletnega mesta (npr. statičnost, dinamičnost in dokumentna ali aplikacijska naravnanost),
- predvidene pogostosti spreminjanja spletne strani,
- tveganja (npr. pravnega, poslovnega).

Za načrtovane spletne dokumente je treba določiti način, čas in pogostost zajema. Vsi ti parametri so lahko za posamezne sklope spletnih dokumentov različni in odvisni predvsem od pogostosti spreminjanja. Zajemamo lahko samodejno ali ročno, in sicer:

- celotno spletno mesto ob vsaki spremembi,
- celotno spletno mesto ob vnaprej določenih časovnih presledkih,
- vsako spremembo ob njeni pojavitvi,
- vsako spremembo, a le če je dovolj pomembna.

Ob zajemu (ali še bolje pred objavo) spletnega dokumenta je treba preveriti ustreznost zapisa. Primer orodja je na spletnem naslovu http://validator.w3.org/ (izvorna koda tega orodja je na voljo za izvajanje validacij v zaprtih okoljih).

Dinamične vsebine[21] so pri dolgoročni hrambi in temu primerni obliki zapisa znatno omejene.

[18] URI – Uniform Resource Identifier.

[19] ZVDAGA, predvsem 40. in 63. člen.

[20] UVDAG, predvsem 11. in 65. člen.

[21] Dinamična vsebina se spreminja glede na čas, vnosna polja in druge parametre. Ta vsebina in prikaz sta nepredvidljiva (ker ne vemo, kaj uporabnik natipka, ne vemo, v kakšni obliki se mu bo stran nato pokazala). Taka stran včasih predstavlja spletni program in vključuje sodelovanje uporabnika po elementih Java skript, ActiveX in drugi logiki odjemalca.

2.3.6 Elektronska pošta[22]

Z izrazom elektronska pošta (e-pošta) označujemo metode izmenjave elektronskih sporočil (e-sporočil). Dolgoročna hramba e-pošte se ne loči od načel hrambe preostalih vrst gradiva. V praksi to pomeni, da moramo e-sporočilo iz lastniške oblike zapisa, ki jo podpira izbrani sistem, pretvoriti v obliko za dolgoročno hrambo, pri tem pa moramo zagotoviti zajem ustreznih metapodatkov. Možnosti so:

- zajem vhodnih e-sporočil,
- zajem izhodnih e-sporočil,
- zajem poštnega predala (npr. ob zaprtju le-tega).

E-pošto opredeljujemo kot nestrukturirani zapis. O eni komponenti govorimo, če je sporočilo shranjeno kot zapis, ki vsebuje telo in vse priponke. Če so priponke shranjene ločeno od telesa e-sporočila, vendar so z njim notranje povezane, je vsaka priponka in telo sporočila komponenta. Če so priponke shranjene ločeno od telesa e-sporočila, vendar z njim niso notranje povezane, je vsaka priponka in telo sporočila ločen dokument. Takrat je treba te dokumente med seboj povezati ročno.

V uporabi je več protokolov za prenos e-pošte. Najpogosteje se uporabljajo tisti, ki jih podpira večina sodobnih odjemalcev in strežnikov, sodelujočih v sistemu izmenjave e-sporočil (SMTP, POP3, IMAP)[23].

Uporabniki lahko uporabljajo različne poštne odjemalce. Ti so lahko povezani v poslovne sisteme e-pošte, ki imajo pogosto lastno notranjo obliko zapisa in lasten notranji protokol za prenos e-sporočil. Tudi komunikacija med strežniki in odjemalci pogosto poteka po nestandardnih protokolih in z uporabo notranjih poštnih prehodov, ki poskrbijo za ustrezno preoblikovanje sporočil.

Programi e-pošte različnih dobaviteljev prosto prenašajo sporočila, ker upoštevajo njene protokole. Pri zajemu e-pošte pa obstaja dvom, ali jo bo drug njen program lahko prebral oz. prikazal enako. Njeni dobavitelji namreč uporabljajo različne lastniške oblike zapisa.

2.3.7 Podatkovne zbirke in uradne evidence

Skupne zahteve za podatkovne zbirke in uradne evidence

Namen zahtev na tem področju je zagotoviti dostopnost, uporabnost, celovitost in pravno veljavnost podatkov v okolju, ki bo neodvisno od izvornega okolja oz. sistema za upravljanje podatkovnih zbirk. To zahteva ohranjanje informacij o organiziranosti podatkovne zbirke, strukturi podatkov, okolju, pravicah uporabnikov, virih podatkov, vmesnikih in spreminjanju vsega naštetega. Zahteve za dokumentacijo tehničnega okolja in programske opreme so opisane že v drugih poglavjih, na tem mestu le poudarimo, da mora dokumentiranost podatkovnega

[22] Področje je opisano v »Študiji dolgoročne hrambe elektronske pošte«, ki je dosegljiva na spletni strani Arhiva RS.

[23] SMTP opredeljuje prenos (oddajo) sporočila in ne njegove vsebine, POP3 (angl. *Post Office Protocol*) je namenjen predvsem prenosu sporočil iz elektronskega nabiralnika do odjemalca e-pošte, IMAP (angl. *Internet Message Access Protocol*) omogoča dostop do nabiralnika e-pošte na oddaljenih strežnikih le-te in odpravlja pomanjkljivosti protokola POP3.

modela omogočati razumevanje medsebojnih povezav posameznih entitet[24] in atributov[25], ki opisujejo entitete in povezave med njimi.

Dodatne zahteve za uradne evidence

ETZ opredeljujejo tudi pogoje za vzpostavitev, upravljanje in vzdrževanje podatkovnih zbirk in na njihovem temelju nastalih uradnih evidenc ter dolgoročno e-hrambo in arhiviranje teh evidenc in podatkov iz navedenih zbirk. V ETZ s pojmom »uradne evidence« označujemo tudi velike registre in evidence javnopravnih oseb.

Za uradne evidence je ob naštetih namenih treba dodati zagotavljanje možnosti vpogleda v staro stanje posameznega zapisa v evidenci na poljuben izbran dan v obdobju njenega vodenja. To načelno velja za vse entitete, a pristojni arhiv lahko omeji izbor entitet, za katere je smiselno voditi zgodovino. Prav tako je treba zagotoviti ohranjanje informacij o vseh pravnih podlagah, ki so opredeljevale upravljanje evidence. Za predpise, ki so javno dostopni, zadošča sklicevanje na javno dostopen uradni vir (Uradni list).

Viri podatkov omogočajo razumevanje, kako je upravljavec uradne evidence pridobival podatke, ki so vneseni vanjo. Vir so lahko izpolnjeni papirni obrazci, druge podatkovne zbirke, od koder so podatki pridobljeni samodejno, osebne izjave pred upravljavcem evidence ipd. Kadar je za izbrano vnosno polje dovoljenih več podatkovnih virov, je treba ta vir za posamezno vrednost dokumentirati.

Pristojni arhiv lahko s pisnim strokovnim navodilom za odbiranje arhivskega gradiva iz dokumentarnega ali z dodatnimi navodili predpiše občasno izdelavo prerezov celotnega stanja evidence ali zgolj sprememb v izbranem obdobju.

2.4. PRETVORBA GRADIVA V OBLIKO ZA DOLGOROČNO E-HRAMBO

Pretvorba je ustrezna, če je celovita in zagotavlja nadaljnjo uporabnost gradiva. Pretvorba v obliko za dolgoročno hrambo se po zakonu obvezno izvaja v primeru arhivskega gradiva in gradiva z rokom hrambe nad 5 let. Prvi pogoj je obstoj možnosti, da izvedemo pravilno pretvorbo iz prvotne oblike zapisa (npr. iz produkcijske). Drugi pogoj je skrb za obstoječe metapodatke, tem pa dodamo ustrezne metapodatke v zvezi s pretvorbo. Tretji pogoj je ciljna oblika zapisa, ki mora ustrezati zahtevam za dolgoročno hrambo, še posebno glede dostopnosti in uporabnosti. Ustrezne oblike zapisa so navadno splošno razširjene, odprte, pregledne in zagotavljajo dolgoročnost, saj je njihova specifikacija javna in reproduktivna ter dajejo zaupanje javnosti, ki dokumente uporablja danes in jih bo tudi v prihodnje. Seznam (nekaterih) oblik[26] zapisa za dolgoročno hrambo posameznih tipov gradiva je v prilogi 1 prvega dela ETZ Uvodna poglavja in priloge.

Organizacija določi oblike zapisa za dolgoročno hrambo, ki jih uporablja, izvaja pretvorbene postopke in vzdržuje programsko orodje. Njihov izbor se bo redko spreminjal, a tudi zato je toliko pomembnejše, da bo odločitev pravilna in pravočasna.

[24] **Entiteta** ali predmet podatkov je objekt opazovanja. Objekt opazovanja pa je vse, kar lahko enolično identificiramo, izoliramo od okolice in opišemo. Entitete identificiramo tako, da jim določimo ime, lastnosti in vrednost teh lastnosti. Entitete so npr. delavec, proizvod, kupec, naročilo.

[25] **Atribut** – entiteto določene vrste opisujemo z lastnostmi oz. atributi. Atribut ali podatkovni element ali element podatkov je tisti podatek, ki z vidika vsebine, torej uporabnika, ni več razstavljiv (ni ga mogoče ali smiselno razstaviti na manjše dele). Atribut je npr. datum rojstva ali matična številka.

[26] Te oblike zapisa morajo zagotavljati dolgoročno dostopnost, kar je najlažje doseči z zahtevami, naštetimi v UVDAG v členu o obliki zapisa za dolgoročno hrambo.

2.5. DOLGOROČNA E-HRAMBA IN ZAVAROVANJE HRANJENEGA GRADIVA PRED IZGUBO

2.5.1 Zagotavljanje avtentičnosti in celovitosti gradiva[27]

Med osnovna načela e-hrambe je vključena zahteva po vzdrževanju celovitosti in avtentičnosti gradiva za celotno obdobje hrambe oz. arhiviranja. Nespremenljivost in celovitost gradiva oz. reprodukcije njegove vsebine je treba zagotavljati verodostojno in preverljivo, zagotavljati pa tudi dokazljivost njegovega izvora (avtentičnosti). Sama narava gradiva v digitalni obliki dopušča razmeroma enostavno neavtorizirano poseganje v vsebino na način, ki onemogoča poznejše evidentiranje takšnih posegov. S takšnim nenadzorovanim poseganjem pa gradivo izgublja avtentičnost izvorne vsebine in tako svojo vrednost. To lahko preprečimo z ustreznimi organizacijskimi ukrepi in tehnološkimi sredstvi, ki nedvoumno in tehnološko preverljivo dokazujejo celovitost in avtentičnost gradiva, dokler traja e-hramba, ne glede na njegov izvor in obliko.

Zahteva po vzdrževanju celovitosti in avtentičnosti velja za gradivo, ki je bilo pretvorjeno v digitalno obliko, oz. za gradivo, ki je izvorno nastalo v digitalni obliki. Poseganje in spreminjanje njegove vsebine omejimo z ustreznimi organizacijskimi ukrepi na ravni upravljanja, uporabe in dostopa do informacijskih virov ter z uporabo ustreznih tehnoloških sredstev za vzdrževanje celovitosti in avtentičnosti. Organizacijski ukrepi dopolnjujejo uporabo teh sredstev tako, da predpisujejo njihovo obliko in način uporabe.

Tehnološka sredstva za zagotavljanje celovitosti gradiva praviloma temeljijo na nadzorovanem dodajanju varnostnih vsebin, ki gradivo spremljajo v celotnem obdobju e-hrambe. To dodajanje je postopek, ki ga mora zagotoviti organizacija pri samem zajemu gradiva. Varnostne vsebine morajo biti ustvarjene tako, da lahko z uporabo vnaprej določenih tehničnih postopkov prikazujejo celovitost in avtentičnost gradiva kadar koli med njegovo hrambo. Tovrstni postopki so zato običajno znani oz. so predmet javne tehnološke standardizacije.

Vzdrževanje varnostnih vsebin (njihove uporabnosti in veljavnosti) moramo zagotavljati v celotnem obdobju e-hrambe. Pred trenutkom njihovega zastaranja moramo zagotoviti njihovo obnavljanje, tako pa podaljšanje uporabnosti in veljavnosti do naslednjega trenutka morebitnega zastaranja. Hkrati moramo zagotoviti možnost izvoza varnostnih vsebin iz sistema skupaj z gradivom. Do takšnih okoliščin pride ob prenosu gradiva med informacijskimi sistemi. Izvorni sistem IUSD mora omogočati izvoz varnostnih vsebin tako, da jih lahko ciljni sistem (sistem, ki sprejme gradivo) ustrezno obdela in zagotovi njihovo vzdrževanje pri nadaljevanju e-hrambe.

Tehnoloških prijemov za zagotavljanje celovitosti in avtentičnosti je več. Glede na uporabljene tehnične postopke in matematične algoritme so ravni zanesljivosti delovanja oz. stopnje zaupanja v varnostne vsebine, ki predstavljajo celovitost in avtentičnost gradiva, različne. Tehnološka sredstva za zagotavljanje celovitosti in avtentičnosti delimo na osnovna in napredna ter jih ločimo tudi glede na to, kakšne prijeme vključujejo za vzdrževanje varnostnih vsebin. S tehnološkim napredkom lahko te izgubljajo uporabnost in zanesljivost, saj je sčasoma z izpopolnjenimi informacijskimi sistemi mogoče manipulirati tudi z (naj)naprednejšimi varnostnimi vsebinami.

Osnovna tehnološka sredstva za vzdrževanje celovitosti in avtentičnosti gradiva v digitalni obliki so tista, ki ne temeljijo na kriptografskih mehanizmih ali ne podpirajo dolgoročnega vzdrževanja veljavnosti varnostnih vsebin za dokazovanje celovitosti in avtentičnosti.

[27] Področje je opisano v študiji z naslovom »Dolgoročno zagotavljanje celovitosti in avtentičnosti gradiva v elektronski obliki«, ki je dosegljiva na spletni strani Arhiva RS.

Predstavljajo manj zanesljive prijeme, ki temeljijo na dodajanju enostavnih varnostnih vsebin in so podprti z dodatnimi organizacijskimi ukrepi pri nadzoru uporabe informacijskih virov, sicer ni mogoče zagotoviti veljavnosti in verodostojnosti varnostnih vsebin. Osnovna tehnološka sredstva temeljijo na postopkih izdelave izvlečkov samostojnih enot gradiva, na podlagi katerih je mogoče prikazati njegovo celovitost. Omejena so s tem, da ne onemogočajo nezaznavnih posegov v varnostno vsebino in da uporabnost oz. veljavnost varnostnih vsebin zaradi tehnološkega napredka s časom propada. Osnovna tehnološka sredstva zato zahtevajo uvedbo dodatnih organizacijskih ukrepov, ki preprečujejo manipulacijo uporabe teh sredstev in neavtorizirane posege v varnostne vsebine.

Med osnovna tehnološka sredstva spadajo: prstni odtis (angl. *message imprint*), elektronski podpis (angl. *digital signature*) in časovni žig (angl. *time stamp*).

Napredna tehnološka sredstva so tista, ki temeljijo izključno na uporabi kriptografskih mehanizmov ter podpirajo dolgoročno vzdrževanje uporabnosti in veljavnosti varnostnih vsebin z občasnim (samodejnim) obnavljanjem in uporabo močnejših kriptografskih mehanizmov. Obnovljene varnostne vsebine ščitijo izvorno gradivo in vse predhodno ustvarjene varnostne vsebine. Obnavljanje je treba zagotoviti pred izničenjem veljavnosti obstoječih varnostnih vsebin. Napredna tehnološka sredstva podpirajo tudi vzdrževanje varnostnih vsebin, ki skupaj z gradivom vstopajo v sistem e-hrambe (elektronski podpisi, časovni žig).

Napredna tehnološka sredstva vključujejo mehanizme za pripravo varnostnih vsebin, ki so tehnološko neodvisni ter katerih priprava in vzdrževanje temelji na javnih mehanizmih in tehnoloških priporočilih. Organizacijski ukrepi morajo navesti najmanj tip in obliko uporabljenih naprednih tehnoloških sredstev.

Med napredna tehnološka sredstva spadajo: napredni digitalni podpis (angl. *Advanced Electronic Signature* – AES) in sintaksa evidenčnih podatkov (angl. *Evidence Record Syntax* – ERS).

2.5.2 Neprekinjeno poslovanje

Izdelava, hramba in uporaba varnostnih kopij gradiva v digitalni obliki

Načelo dostopnosti[28] med drugim zahteva, da mora biti gradivo oz. reprodukcija njegove vsebine *»ves čas trajanja hrambe zavarovana pred izgubo«*. To zavarovanje se v organizacijah uresničuje predvsem z izdelavo in hrambo varnostnih kopij[29] gradiva na drugih, oddaljenih mestih (sekundarnih lokacijah). Pogostost izdelave kopij, njihovo število ter število in oddaljenost mest za njihovo hrambo mora biti postavljena na podlagi ocene tveganja. Ta mora upoštevati obseg, občutljivost in kritičnost gradiva v hrambi ter značilnosti uporabljene tehnologije. Raven varovanja varnostnih kopij gradiva na oddaljenih mestih mora biti enaka ravni njegovega varovanja na primarnem (glavnem) mestu hrambe. V ta namen mora organizacija izdelati načrt za obnovo podatkov na glavnem mestu iz njihovih varnostnih kopij, shranjenih na oddaljenem oz. oddaljenih mestih. Postopek obnove podatkov iz varnostnih kopij

[28] ZVDAGA, 6. člen.

[29] UVDAG, 5. člen/prvi odstavek, točka 3i: notranja pravila morajo v zvezi z infrastrukturo informacijskega sistema za hrambo vsebovati določbe o nepretrganem poslovanju. Organizaciji je prepuščeno, kakšna bo raven zagotavljanja nepretrganosti poslovanja.

UVDAG, 5. člen/četrti odstavek, točka 4: notranja pravila o hrambi arhivskega gradiva morajo vsebovati še najmanj določbe o **zagotavljanju** nepretrganega poslovanja oz. varstva arhivskega gradiva in njegovi izročitvi pristojnim arhivom. V tem primeru je torej zahtevano zagotavljaje nepretrganega delovanja, kar pomeni, da mora biti sistem za e-hrambo oblikovan tako, da bo preprečena kakršnakoli možnost izgube hranjenega arhivskega gradiva, medtem ko čas okrevanja sistema po morebitni katastrofi z vidika ZVDAGA ni (tako) pomemben.

je praviloma del okrevalnega načrta (načrta za obnovo podatkov) informacijskega sistema za e-hrambo podatkov (angl. *Disaster Recovery Plan* – DRP).

Dodatne zahteve za javnopravne osebe in ponudnike storitev e-hrambe

Če organizacija hrani pomembnejše gradivo, med katero spada tudi arhivsko, pa zakon zahteva od nje, da načrtuje in izvaja ukrepe za neprekinjeno delovanje infrastrukture informacijskega sistema za hrambo. Med te organizacije spadajo javnopravne osebe kot ustvarjalci arhivskega gradiva in ponudniki storitev e-hrambe, ki morajo sprejeti načrt neprekinjenega poslovanja (delovanja) sistema za e-hrambo (angl. *Business Continuity Plan*), ki mora temeljiti na oceni tveganja. Sestavni del tega načrta je tudi načrt za obnovo podatkov.

Ponudnik storitve e-hrambe mora pri ukrepih in postopkih za zavarovanje gradiva pred izgubo ali poškodovanjem poleg hrambe varnostnih kopij zagotavljati tako raven neprekinjenega delovanja sistema za e-hrambo, ki bo ustrezala obsegu in kakovosti, h katerima se je pogodbeno zavezal. Razpoložljivost tega sistema, ki ga ponuja na trgu, mora biti skladna s pogodbeno določeno ravnijo storitve (angl. *Service Level Agreement* – SLA). Na primer: če ponudnik naročniku obljubi dostop 24 x 365 do storitve e-hrambe oz. dostop do hranjenega gradiva, mora biti razpoložljivost nadomestne infrastrukture skladna z opredeljenim najdaljšim obdobjem okrevanja iz NP oz. pogodbe o izvajanju storitve e-hrambe, v katerem morajo biti infrastruktura, programi oz. evidence informacijskega sistema za hrambo po nenačrtovanem izpadu obnovljeni (npr. ena ura, en delovni dan; angl. *Recovery Time Objective* – RTO). V tej pogodbi mora biti določena tudi kritična obnovitvena točka (angl. *Recovery Point Objective* – RPO) kot skrajni rok, do katerega je treba vzpostaviti ponovno delovanje funkcij izpadlega informacijskega sistema za e-hrambo.

V predhodni raziskavi, analizi poslovnega delovanja in oceni tveganja mora ponudnik opredeliti raven svoje storitve ter temu primerno dimenzionirati opremo in infrastrukturo sistema za e-hrambo na primarnem in po potrebi (beri: če želi tržiti storitev e-hrambe, kjer to predpisi izrecno zahtevajo) na oddaljenem mestu hrambe.

2.6. ODBIRANJE IN IZROČANJE ARHIVSKEGA GRADIVA V DIGITALNI OBLIKI TER SODELOVANJE S PRISTOJNIM ARHIVOM

ZVDAGA določa, da javno arhivsko gradivo hranijo le pristojni arhivi[30]. Zato morajo vse organizacije, katerih dokumentarno gradivo je bilo v skladu z navodili pristojnega arhiva spoznano za arhivsko, to gradivo arhivom tudi izročiti. Arhivsko gradivo v digitalni obliki se lahko izroča le v obliki za dolgoročno hrambo, v kakršni koli drugi obliki pa le s soglasjem državnega arhiva. Javnopravne osebe lahko pod določenimi, z zakonom[31] opredeljenimi pogoji same hranijo svoje arhivsko gradivo. Nekoliko drugačne določbe veljajo za zasebno arhivsko gradivo. To je last fizičnih in pravnih oseb zasebnega prava, te pa ga ob izpolnjenih zakonskih pogojih[32] lahko hranijo same ali ga izročijo v hrambo pristojnemu arhivu.

ZVDAGA določa, da filmsko in avdiovizualno arhivsko gradivo prevzema Arhiv RS, sektor Slovenski filmski arhiv. Z ustvarjalci oz. producenti filmskega in avdiovizualnega arhivskega gradiva v digitalni obliki se glede oblike in formata izročanja v arhivsko dolgoročno hrambo dogovori v okviru posameznega prevzema.

[30] ZVDAGA, 36. člen.
[31] ZVDAGA, 62. člen.
[32] ZVDAGA, 45. člen.

V nadaljevanju navajamo primer, ki se nanaša na nosilce zapisov, na katerih se v tem času izroča arhivsko gradivo v digitalni obliki v pristojne arhive:

Primer 1:

Arhivsko gradivo na mikrofilmu se izroča v teh oblikah:

- *arhivsko gradivo, katerega izvorna oblika je večja od formata A3 (npr. tehnična dokumentacija, časopisi, karte, knjige), se izroča na mikrofilmu v zvitku širine 35 mm;*
- *s predhodno pridobljeno potrditvijo Arhiva RS se lahko arhivsko gradivo izroča tudi na mikrofilmu v zvitku širine 16 mm;*
- *mikrofiš formata A6 8148 X 105 mm.*

2.7. IZLOČANJE IN UNIČEVANJE DOKUMENTARNEGA GRADIVA

Izločamo tisto gradivo, ki ga nameravamo uničiti. Uničenje je postopek odstranitve ali brisanja, tako da rekonstrukcija gradiva pozneje ni več mogoča.

Glede na določila UVDAG[33], ki opredeljujejo obvezno vsebino NP, mora vsaka organizacija določiti postopek izločanja in uničevanja dokumentarnega gradiva. Za javnopravne osebe pa ta postopek še posebno podrobno opredeljuje UVDAG[34].

Uničenje gradiva v digitalni obliki, ki mu je potekel rok hrambe, je lahko samodejno (ISUD) ali ročno, v obeh primerih pa na podlagi odločitve pristojne osebe. Postopek uničenja je odvisen od vrste gradiva (oblike in vsebine). Pri zajemu iz fizične v digitalno obliko lahko gradivo v fizični obliki uničimo, v digitalni obliki pa mu ohranimo enakost z izvirnim gradivom na podlagi ZVDAGA.[35] To pa velja le, če je bil zajem opravljen na podlagi notranjih pravil, ki jih je potrdil državni arhiv in jih je organizacija dokazljivo izvajala (notranja oz. zunanja presoja njihovega izvajanja).

V skladu s predpisi, ki urejajo varovanje osebnih in tajnih podatkov, poslovne in davčne tajnosti ipd., mora izločanje in uničevanje obsegati uničenje vseh kopij, vključno z varnostnimi (izbris elektronske oblike in uničenje neuporabnih medijev, na katerih je bilo gradivo shranjeno), na vseh mestih, kjer so se hranile.

3. INFORMACIJSKA VARNOST

Pojem »informacijska varnost« v ETZ obsega organizacijske in tehnične ukrepe ter postopke varne hrambe izvirnega, zajetega ali pretvorjenega gradiva. Namen izvajanja ukrepov in postopkov informacijske varnosti je:

- varovanje gradiva pred njegovo izgubo, nepooblaščenimi spremembami ali nepooblaščenim razkritjem,
- omejevanje dostopa do shranjenega gradiva na pooblaščene uporabnike,
- zagotavljanje varnosti in razpoložljivosti informacijskih sistemov za zajem in e-hrambo oz. s tem povezane spremljevalne storitve,
- zagotavljanje pravne veljavnosti e-hranjenega gradiva, kar omogoča uporabo tega gradiva kot dokazila v različnih uradnih postopkih.

[33] UVDAG, 5. člen.

[34] UVDAG, 72. in 73. člen.

[35] ZVDAGA, 13.–16. člen, 31. člen.

Za doseganje načel varne e-hrambe moramo zagotoviti ukrepe in postopke, s katerimi bomo varovali gradivo pred njegovo *izgubo* in *okrnitvijo* ter *dokazovanjem celovitosti:*

- Prvo zahtevo, ki se nanaša na preprečevanje *izgube*, izpolnjujemo z ustreznim številom varnostnih kopij gradiva na različnih mestih, s prepisovanjem njegove vsebine na nove nosilce zapisa, preden obstoječi propadejo, s stalnim preverjanjem nosilcev zapisa in s pravočasno pretvorbo gradiva iz ene obliko zapisa v drugo pred zastaranjem oblike, v kateri je hranjeno.
- Drugo zahtevo, ki se nanaša na varovanje pred *okrnitvijo in dokazovanjem celovitosti* gradiva ter obsega zagotavljanje njegove točnosti, nespremenljivosti in popolnosti oz. reprodukcije njegove vsebine in dokazljivosti njegovega izvora ves čas hrambe, pa izpolnjujemo s tvorbo in hrambo ustreznih metapodatkov in revizijskih sledi o zajemu, pretvorbi, popravkih ali dopolnitvah hranjenega gradiva.[36]

Gradivo oz. reprodukcija njegove vsebine sme biti ves čas trajanja hrambe *dostopno* (le) *pooblaščenim uporabnikom.* Zahteva po omejevanju dostopa obsega tudi[37]:

- omejevanje dostopa do prostorov, v katerih sta oprema in infrastruktura informacijskega sistema za zajem in e-hrambo,[38]
- omejevanje dostopa do prostorov, v katerih se hranijo nosilci zapisov gradiva oz. v katerih je nameščena oprema informacijskega sistema za zajem in e-hrambo,[39]
- varnostne ukrepe in postopke v zvezi z osebjem, ki sodeluje pri zajemu in e-hrambi.[40]

Za delovanje informacijskega sistema za zajem in e-hrambo je pomembno tudi zagotavljanje potrebne okoljske varnosti.

Zgornje navedbe o hrambi arhivskega gradiva oz. gradiva javnopravnih oseb spadajo v t. i. *materialno varstvo* gradiva.[41]

3.1. POPIS IN VARNOSTNA RAZVRSTITEV INFORMACIJSKIH VIROV

Temelji za ustrezno upravljanje in varovanje gradiva so jasno opredeljene odgovornosti za varovanje posameznega informacijskega vira. Glede na njegovo občutljivost in zaupnost ga varnostno razvrstimo (klasificiramo).

3.1.1 Popis informacijskih virov

Identificirati in popisati je treba vse pomembnejše informacijske vire, ki so povezani s postopki upravljanja gradiva, zajema in njegove e-hrambe.

Med informacijske vire spadajo:

- *informacijska sredstva:* podatkovne zbirke, datoteke, sistemska dokumentacija, uporabniški priročniki, gradivo za usposabljanje, obratovalni postopki, načrti za neprekinjeno delovanje itd.;

[36] UVDAG, 11., 12. in 13. člen.

[37] Podrobneje to zahtevo urejajo določbe ZVDAGA, 23., 26., 27., 68. in 71. člen, ter UVDAG, 5.,16. in 22. člen.

[38] UVDAG, 5., 16. in 22. člen.

[39] UVDAG, 5., 16. in 22. člen.

[40] UVDAG, 5. člen.

[41] ZVDAGA, 36., 39. in 53. člen; UVDAG, 39. in 40. člen.

- *programska oprema:* popis obstoječe programske opreme (seznam, dostopi, pooblastila ...), kamor prištevamo aplikacijsko in infrastrukturno programsko opremo, razvojno orodje in podporne programe itd.;
- *fizična sredstva*: računalniška in komunikacijska oprema (strojna oprema), nosilci podatkov, druga tehnična oprema, prostori itd.;
- *storitve računalniškega obdelovanja in komunikacijske storitve ter druge tehnične storitve* (npr. elektrika, hlajenje, fizično varovanje).

Tako npr. mora organizacija v NP navesti vsaj te podatke o strojni opremi: tip strojne opreme, proizvajalca, serijo oz. model (glej tudi ETZ 4.2.1.1); o programski opremi: identifikacijsko oznako oz. ime, oznako različice in vse dodatne komponente, ki sestavljajo programsko opremo in predstavljajo njeno določeno funkcionalnost (glej tudi ETZ 4.4.2.4).

3.1.2 Odgovorne osebe za varovanje informacijskih virov

Organizacija mora določiti skrbnike (lastnike) posameznih informacijskih virov oz. skupin virov, ki so odgovorni za njihovo uporabo in obravnavanje v skladu s predpisanimi oz. pogodbeno določenimi zahtevami, pravili in standardi. Skrbniki so praviloma vodje organizacijskih enot, v katerih pristojnost spada posamezna vrsta gradiva, deli informacijske infrastrukture sistema za zajem oz. e-hrambo ali posamezni zaposleni v teh organizacijskih enotah.

3.1.3 Varnostna razvrstitev informacijskih virov

Organizacija mora evidentirane informacijske vire varnostno razvrstiti v skladu z veljavnimi pravnimi zahtevami, oceno tveganja in kritičnostjo oz. občutljivostjo gradiva, ki ga zajema oz. hrani. Varnostna razvrstitev teh virov je podlaga za določanje ukrepov in postopkov za varno, nadzorljivo in sledljivo uporabo oz. obravnavanje informacijskih virov ter izvajanje potrebnih varnostnih ukrepov.

3.2. ORGANIZIRANJE INFORMACIJSKE VARNOSTI

Organizacija mora pri pripravi oz. organiziranju zajema in e-hrambe izpolniti vse predpisane varnostne zahteve, bistvene za posamezno vrsto gradiva (npr. dokumentarno gradivo; arhivsko gradivo; gradivo v fizični ali digitalni obliki) oz. vrsto podatkov, ki jih bo vsebovalo zajeto oz. hranjeno gradivo (osebni, tajni, zaupni, javni ipd. podatki).

Iztočnica za načrtovanje, organiziranje in izvajanje varovanja gradiva je *ocena tveganja* pri zajemu oz. e-hrambi. Na njeni podlagi organizacija določi, vzpostavi in izvaja ukrepe ter postopke varovanja gradiva in delovnih postopkov ter opreme za zajem oz. e-hrambo.

Organizacija mora zagotavljanje informacijske varnosti urediti z NP. Pri tem mora upoštevati predpise, ki določajo način varovanja podatkov v zajetem oz. hranjenem gradivu. Med pomembnejšimi predpisi je Zakon o varstvu osebnih podatkov (ZVOP–1)[42], saj pravzaprav ni organizacije, pri kateri vsaj del zajetega oz. e-hranjenega gradiva ne bi vseboval tudi osebnih podatkov. Sprejetje notranjega akta kot podlage za organiziranje sistema informacijske varnosti zahteva 25. člen ZVOP-1 (npr. Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov), poleg njega pa številni drugi predpisi, ki urejajo obdelavo manj pogostih ali na določena področja omejenih vrst podatkov (npr. 38. člen Zakona o tajnih podatkih za tajne

[42] ZVOP-1 v 25. členu od organizacij zahteva, da *»v svojih aktih predpišejo postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke«*.

podatke, 42. člen Zakona o državni statistiki za statistično tajnost, 17. člen Zakona o davčnem postopku za davčno tajnost, 54. člen Zakona o maturi za izpitno tajnost).

Določbe za organiziranje, vzpostavitev in upravljanje sistema informacijske varnosti v organizaciji morajo temeljiti na določbah ZVDAGA in drugih pravnih predpisov, ki se morajo upoštevati glede na vrsto zajetega oz. hranjenega gradiva. Pri pripravljanju ukrepov in postopkov informacijske varnosti ter aktov o ureditvi sistema te varnosti si organizacije lahko pomagajo s standardi, priporočili in dobrimi praksami s tega področja (npr. ISO 27001[43] in ISO 27002[44]).

3.2.1 Ocena tveganja

Ukrepi in postopki informacijske varnosti morajo temeljiti na oceni tveganja, ki jo mora organizacija izdelati že v predhodni pripravi na zajem in e-hrambo. Ta ocena je zgolj podlaga za izvajanje zajema oz. vzpostavitev varnega sistema e-hrambe ter podlaga za poznejše upravljanje tveganja, zato da se gradivo ustrezno zavaruje med hrambo. Tveganje je možnost (verjetnost), da bo informacijski vir ali skupina virov ogrožena[45] zaradi svoje ranljivosti[46] in da bo povzročena izguba oz. škoda na njih.

Tveganja so lahko različna:

- *Pravna in poslovna tveganja* (najem zunanjih izvajalcev, tveganja, ki izvirajo iz notranje in zunanje organizacije, tveganja, povezana s skladnostjo s predpisi, itd.). Glede ocene pravnega tveganja organizacija določi zakone in druge predpise, ki jih mora spoštovati pri zajemu oz. e-hrambi glede na vrsto gradiva oz. vrsto podatkov, ki jih to gradivo vsebuje.
- *Tveganja, povezana s človeškimi viri* (nenamerna/namerna dejanja, usposobljenost osebja, pristojnosti in odgovornosti osebja itd.).
- *Tveganja, povezana z okoljem:*
  - netehnološka tveganja (požar, izlitje vode, naravne ujme /poplava, neurje, potres, požar v okolju, vihar, vročina, strela/, teroristični napad itd.),
  - tehnološka tveganja (povezana z informacijsko tehnologijo, npr. odpoved delovanja, zastaranje strojne in programske opreme, zastaranje nosilcev[47] podatkov, zastaranje oblik[48] zapisa itd.).
- *Druga tveganja, povezana tudi z informacijsko varnostjo in izvajanjem e-hrambe* (tveganja, povezana z upravljanjem sprememb informacijske tehnologije in sistemov, itd.).

Izdelava ocene tveganja mora temeljiti na metodologijah[49], ki omogočajo naknadno preverjanje ugotovitev ocene in njeno poznejše posodabljanje. V nadaljevanju je naveden kratek primer izdelave ocene tveganja.

[43] Objave št. 7/2006 Slovenskega inštituta za standardizacijo; SIST ISO/IEC 27001:2006 je enakovreden ISO/IEC 27001:2005.

[44] Objave št. 5/2008 Slovenskega inštituta za standardizacijo; SIST ISO/IEC 27002:2008 je enakovreden ISO/IEC 27002:2005.

[45] Ogroženost je zunanji vpliv, ki lahko izkoristi ranljivost sredstva in povzroči škodo sredstvu, sistemu ali organizaciji.

[46] Ranljivost je slabost sredstva ali skupine sredstev, zaradi katere so lahko ogrožena.

[47] Za zdaj velja, da so elektronski nosilci podatkov manj obstojni od papirja. Občutljivost nosilcev in njihovo propadanje lahko povzročita izgubo ali uničenje gradiva.

[48] Obstaja npr. nevarnost, da z uvajanjem nove programske opreme izgubimo možnost prikazati gradivo v kakšni od starejših oblik (formatov) zapisa, če ne bomo pravočasno poskrbeli za pretvorbo gradiva v drugo obliko.

Za vsak informacijski vir v izbranem obsegu poslovnih postopkov in sistema e-hrambe:

- ugotovimo, kaj bi ta vir lahko ogrozilo,
- prepoznamo ranljivost vira za konkretno nevarnost,
- ocenimo posledice, če bi se grožnja uresničila.

Pri tem si smiselno pomagamo tudi s podatki o preteklih varnostnih incidentih, strokovnimi mnenji, ugotovitvami varnostnih pregledov, izkušnjami drugih itd. Na podlagi kritičnosti/pomembnosti[50] tveganja in verjetnosti[51], da se bo grožnja uresničila (npr. na lestvici od 1–5), določimo stopnjo tveganja. Vsako tveganje ovrednotimo in opredelimo kot *sprejemljivo* (npr. stopnje 1–3) ali *nesprejemljivo* (npr. stopnji 4 in 5). Sprejemljiva tveganja mora vodstvo pisno odobriti, lastniki poslovnih postopkov pa morajo za zmanjšanje tveganja določiti preprečevalne ukrepe. Za vsako nesprejemljivo tveganje določimo:

- ukrepe, npr. tehnične in organizacijske, za zmanjšanje tveganja na sprejemljivo raven;
- rok izvedbe ukrepa in odgovorno osebo.

Ukrepe moramo nato izvesti in oceno tveganja posodobiti. Ocena tveganja namreč ni enkratno dejanje, temveč stalen proces, ki zajema oceno[52] tveganj, njihovo obvladovanje[53] in njihovo redno preverjanje[54].

3.2.2 Notranje pravna ureditev informacijske varnosti

Odločitev o formalni obliki notranje pravne ureditve informacijske varnosti je odvisna predvsem od ugotovitev ocene pravnega tveganja, po katerih se organizacija odloči, ali bo to področje uredila:

1. neposredno z besedilom NP oz. s posebnim aktom o (za)varovanju zajema oz. e-hrambe (npr. s pravilnikom, poslovnikom, navodilom, politiko informacijske varnosti);
2. z ustrezno dopolnitvijo obstoječih aktov organizacije s področij:
   - (za)varovanja podatkov (npr. pravilnika o zavarovanju osebnih podatkov, o zavarovanju tajnih podatkov, o zavarovanju poslovnih skrivnosti),
   - urejanja drugih varnostnih vprašanj (npr. požarne varnosti, hišnega reda ipd.),
   - organiziranosti ter opisa del in nalog zaposlenih (npr. akt o organizaciji in sistemizaciji delovnih mest),
   - upravljanja dokumentarnega gradiva (npr. pravilnik o pisarniškem poslovanju) ipd.

Vsebina aktov oz. dokumentov, s katerimi organizacija uredi informacijsko varnost, je odvisna od ugotovitev ocene tveganja, varnostne razvrstitve informacijskih virov ter organiziranosti in področja poslovanja organizacije.

---

[49] Za pomoč pri določanju smernic za obvladovanje tveganja glede informacijske varnosti lahko uporabite kakšnega izmed standardov s tega področja, npr. ISO/IEC 27005 (podpira varnostne kontrole, opredeljene s standardom ISO/IEC 27001), del metodologije COBIT (Control Objectives for Information and Related Technology), metodologijo CoCo in metodologijo vrednotenja COSO (Committee of Sponsoring Organisation).

[50] *Kritičnost/pomembnost tveganja:* za vsako zaznano tveganje določimo njegovo kritičnost oz. pomembnost, npr. v razponu od »nična« (uresničitev grožnje ne prizadene delovanja sistema in varnosti gradiva) do »zelo visoka« (uresničitev grožnje ima katastrofalne posledice za sistem in za gradivo).

[51] *Verjetnost tveganja:* verjetnost, da se grožnja uresniči, in možnosti, da jo pravočasno odkrijemo, npr. z lestvico od 1 (glede na izkušnje je nemogoče, da bi se pojavila napaka) do 5 (verjetnost uresničitve grožnje je brez ukrepov zelo visoka in zelo pogosta; možnosti, da grožnjo pravočasno odkrijemo, pravzaprav ni). Vmesne stopnje določimo glede na pogostost uresničitve grožnje in možnost njenega pravočasnega odkritja.

[52] Angl. *Risk Assessment*.

[53] Angl. *Risk Control*.

[54] Angl. *Risk Review*.

Če organizacija sprejme politiko informacijske varnosti[55] kot samostojno dokumentacijo, je ta sestavni del NP. Navadno jo sestavljajo krovni dokument na najvišji ravni in področne varnostne politike na drugi ravni, ki jih dopolnjujejo različna navodila, obrazci in notranji standardi na tretji ravni.
V *krovnem dokumentu politike informacijske varnosti* se zapišejo obvezujoča pravila in predpisi, ki se nanašajo na splošna načela upravljanja informacijskega sistema, npr.:

- namen in cilj varnostne politike,
- odgovornosti (vodstva, zaposlenih, tretjih oseb),
- odgovorne osebe za informacijsko varnost in njeno izvedbo,
- usklajenost (npr. s predpisi, tehnologijo),
- način in pogostost preverjanja in dopolnjevanja varnostne politike,
- način obravnavanja varnostnih incidentov[56] pri varovanju informacij (kršenje politike in disciplinski ukrepi),
- organizacija dokumentacije, ki predstavlja politiko informacijske varnosti in se nanaša na posamezna področja,
- veljavnost.

V *področnih varnostnih politikah* pa so natančneje opredeljene zahteve po uvedbi varnostnih ukrepov in postopkov varovanja na posameznih področjih, ki morajo izhajati iz ocene tveganja ter odgovornosti za izvedbo, način uvedbe in nadzor nad njimi. Z vidika zahtev po varovanju, kakršne določa ZVDAGA, lahko opredelimo področne varnostne politike, ki se npr. nanašajo na: varovanje v zvezi z osebjem, upravljanjem informacijskih virov in informacijske infrastrukture ter operativnega delovanja, s fizičnim in tehničnim varovanjem, z upravljanjem dostopnih pravic, naročanjem storitev pri zunanjih izvajalcih in neprekinjenim poslovanjem.

Za organiziranje in izvajanje ukrepov ter postopkov informacijske varnosti mora organizacija imenovati odgovorno osebo (vodjo informacijske varnosti), katere naloge so predvsem:

- nadzor stanja informacijske varnosti,
- odrejanje ukrepov za zagotavljanje informacijske varnosti,
- nadzor nad upravljanjem in izvajanjem varnostnih ukrepov in postopkov pri zagotavljanju informacijske varnosti,
- vodenje razvida informacijskih varnostnih incidentov,
- vodenje seznamov oseb, pooblaščenih za samostojen vstop v prostore, v katerih so nameščene ključne naprave sistema za zajem oz. e-hrambo,
- vodenje seznamov oseb, pooblaščenih za dostop do hranjenega gradiva,
- sodelovanje pri sistemih za upravljanje identitet in dostopnih pravic uporabnikov sistema za zajem oz. e-hrambo.

Zaposleni v organizaciji (redno in začasno) in morebitni zunanji sodelavci morajo podpisati izjavo o zaupnosti oz. varovanju informacij. S podpisom te izjave potrdijo, da so seznanjeni s predpisi in akti, ki v organizaciji urejajo varovanje gradiva in njegove vsebine kot predmeta zajema in e-hrambe.

Dodatne zahteve za javnopravne osebe in ponudnike storitev

[55] Sinonim je še: informacijska varnostna politika, Pravilnik o varovanju informacij. Politika informacijske varnosti je del sistema upravljanja informacijske varnosti (SUIV, angl. *Information Security Management System* – ISMS).

[56] **Varnostni incident** – vsak dogodek, ki je v nasprotju z informacijsko varnostno politiko organizacije (npr. poskus nepooblaščenega dostopa do podatkov). Obvladovanje varnostnih incidentov obravnava tudi standard ISO/IEC TR 18044:2004 – Information technology – Security techniques – Information security incident management.

Uredba o upravnem poslovanju nekatere javnopravne osebe zavezuje k vzpostavitvi sistema upravljanja informacijske varnosti (SUIV)[57], vključno z izdelavo politike informacijske varnosti, skladno s priporočili ministrstva, pristojnega za javno upravo. Vzpostavitev in dokumentiranje SUIV se zahteva tudi od ponudnikov storitev zajema in e-hrambe, saj jih lahko ponujajo javnopravnim osebam, ki hranijo arhivsko gradivo.
SUIV je sistem, na podlagi katerega organizacija vpelje, nato pa vzdržuje in nenehno izboljšuje informacijsko varnost. Obseg in meje SUIV določi na podlagi odločitve (dokumentirane) odgovorne osebe oz. vodstva, pri čemer mora upoštevati značilnosti lastne organiziranosti, poslovanja in kraja poslovanja ter zahteve veljavnih predpisov.

Delovanje SUIV mora temeljiti na izvedeni oceni tveganja, ki je podlaga za izbiro ustreznih nadzorstev oz. ukrepov za zagotavljanje nemotenega delovanja storitve ponudnika. Obseg SUIV mora biti določen tako, da vključuje vse subjekte in dejavnosti v zvezi z zajemom in e-hrambo gradiva (lastnega in tujega). Določen je tudi glede na organizacijske dele, ki bodo zajeti v SUIV, postopke, ki se bodo varovali, ljudi, ki nastopajo v postopkih, informacijsko infrastrukturo in komunikacijo, vire in storitve.

Dokumentacijo SUIV predstavljajo:
- krovna politika informacijske varnosti,
- področne varnostne politike,
- navodila, obrazci, postopki za posamezna področja,
- zapisi, s katerimi se dokumentirano dokazuje izvajanje postopkov v sistemu varovanja informacij in tako skladnost z zahtevami ZVDAGA (npr. logi, zapisi, revizijske sledi).

3.3. FIZIČNO IN TEHNIČNO VAROVANJE PROSTOROV IN OPREME

Prostori (varovana območja), v katerih je nameščena oprema za zajem in e-hrambo oz. v katerih se ta izvaja, vključno z morebitnimi spremljevalnimi storitvami, morajo biti varovani pred nepooblaščenim vstopom, okoljskimi nevarnostmi (npr. požar, izlitje vode) ter biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi, in sicer tako, da je omogočen dostop zgolj pooblaščenim uporabnikom in da gradivo ni ogroženo.

3.3.1 Določitev prostorov za zajem in e-hrambo ter njihovo varovanje

Na varovana območja nameščamo ključno opremo sistema za zajem in e-hrambo (npr. strežnike, spominske enote, komunikacijske naprave, šifrirne naprave). Prostori varovanega območja, v katerih se izvaja dodaten nadzor nad dostopom oseb in tehnično varovanje, so navadno sistemski prostor in drugi prostori z instalacijami in komunikacijami, pomembnimi za organizacijo. Za varovana območja mora organizacija zagotoviti ustrezne varnostne ukrepe, npr.:

- namestitev protipožarnih vrat,
- samodejna vstopna kontrola,
- videonadzor vstopa na varovana območja,
- samodejni izklop elektrike,
- namestitev javljalnikov požara in vzpostavitev postopkov rednega preverjanja njihovega delovanja ter vodenje dnevnikov preizkusov,
- namestitev samodejnega protipožarnega sistema na najobčutljivejših varovanih območjih,
- namestitev javljalnikov izlitja vode in samodejnih črpalk.

[57] UUP, 80. člen.

Pri načrtovanju in izvajanju varnostnih ukrepov in postopkov na varovanih območjih mora organizacija, poleg določb ZVDAGA in UVDAG, upoštevati zahteve drugih ustreznih predpisov (npr. izdelava požarnega reda, požarnega načrta in evakuacijskega načrta po predpisih o požarni varnosti; izdelava in sprejetje izjave o varnosti po predpisih o zagotavljanju zdravja in varnosti pri delu).

3.3.2 Varovanje vstopanja v prostore za zajem in e-hrambo

Vstop posameznikov na varovana območja mora izhajati iz njihovih nalog. Izveden mora biti tako, da je omogočen nadzor nad vstopanjem oz. izstopanjem zaposlenih ter drugih pooblaščenih oseb in obiskovalcev na varovana območja oz. z njih. Če se na varovanem območju zajema oz. elektronsko hrani gradivo, ki vsebuje zaupne podatke (občutljive osebne podatke, tajne podatke, davčno tajnost, bančne zaupne podatke, poslovne skrivnosti ali druge vrste posebej varovanih podatkov), mora biti gibanje na tem območju urejeno v skladu s predpisi, ki določajo njihovo varovanje.

Vstop drugih oseb na varovano območje mora odobriti pristojna oseba in mora biti evidentiran, njihovo gibanje pa morajo ustrezno nadzirati zaposleni oz. druge pristojne osebe.

Vstop na varovano območje se nadzira z ugotavljanjem identitete vstopajočega. Vstopna kontrola je lahko fizična ali tehnična, temelji lahko na sistemu samodejnega prepoznavanja identifikacijskih kartic oz. biometričnih značilnosti vstopajočih.

Zapisi v evidenci vstopov zaposlenih in drugih oseb na varovana območja morajo biti občasno preverjeni za ugotavljanje morebitnih kršitev vstopnih pravil.

3.4. UPRAVLJANJE DOSTOPNIH PRAVIC DO SISTEMA IN GRADIVA

Zaposlenim je treba, po pravilu minimalne pravice, zagotoviti takšen dostop do podatkov in informacij, da jim je omogočeno izvajanje delovnih nalog oz. obveznosti. Hkrati je treba preveriti, ali informacije, do katerih dostopajo, dejansko potrebujejo iz utemeljenega razloga. Ključno vlogo pri tem imajo skrbniki informacijske rešitve oz. gradiva, ki morajo informacije že ob nastanku ustrezno varnostno razvrstiti in tako določiti njihovo dostopnost.

Vsak skrbnik informacijske rešitve oz. gradiva naj opredeli, dokumentira in vzdržuje jasna pravila dostopa, s katerimi določa dostopne pravice posamezniku ali skupini uporabnikov in predpiše:

- kakšne so varnostne zahteve pri uporabi posameznih informacijskih rešitev oz. gradiva,
- kdo je pooblaščen in kdo mora biti seznanjen s temi pravili dostopa.

Pri dodeljevanju dostopnih pravic do informacijskih sistemov in gradiva je smiselno, če je glede na velikost organizacije le mogoče, upoštevati tudi pravilo razdelitve (ločevanja) nalog tako, da posameznik nima takšnih pooblastil, da bi lahko neopaženo kompromitiral ali zlorabil informacije oz. gradivo, do katerega ima dostop.

Vsako obliko obdelave gradiva je treba evidentirati z revizijsko sledjo, ki omogoča naknadno rekonstrukcijo dostopa. Pri tem je treba upoštevati tudi določbe Zakona o varstvu osebnih podatkov, katerega namen je preprečevati nezakonite in neupravičene posege v zasebnost posameznika pri obdelavi osebnih podatkov, njihovem varovanju in uporabi.

Politiko omejevanja dostopa lahko organizacija izvaja npr. z dodeljevanjem enoličnih uporabniških imen in pripadajočih gesel, uporabi pa lahko še druge identifikatorje (npr. pametne kartice z digitalnimi potrdili, generatorje žetonov za enkratno prijavo, biometrične podatke). Z dodelitvijo takih imen in gesel oz. identifikatorjev ter s prepovedjo njihovega posojanja drugim

bo vedno mogoče ugotoviti, kdo je v nekem času dostopal do informacijskega sistema oz. gradiva. Uporabniške pravice za te dostope je treba ves čas nadzorovati in skrbeti za njihovo posodobitev. Prav tako je treba vzpostaviti formalni postopek njihovega pregledovanja.

3.4.1 Postopek dodelitve, spreminjanja in odvzema uporabniških pravic

Vzpostaviti je treba tudi formalni postopek upravljanja dostopnih pravic do sistemov za zajem in e-hrambo ter odgovornosti glede na delovne naloge. Še posebno je treba upoštevati različne vrste zaupnih podatkov (npr. Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih). Postopek naj vključuje dodeljevanje dostopnih pravic in njihovo odvzemanje ter vodenje evidence. Jasno mora biti opredeljeno, kdo ima dostop do določenih podatkov in katere informacijske varnostne zahteve so potrebne za posamezne informacijske rešitve v organizaciji.

Dodeljevanje pravic za dostop do posameznih informacijskih sistemov in gradiva bo učinkovito, uspešno in varno, če bodo jasno opredeljeni:

- postopek dodeljevanja dostopov,
- odgovornosti,
- razvrstitev gradiva,
- informacijske storitve, do katerih je dovoljen dostop,
- dovoljeni načini dostopa do informacijskih storitev,
- nastavitve programske in strojne opreme, ki omogočajo varno uporabo informacijskih storitev,
- dostopni profil za vsakega uporabnika, ki naj določa, katere storitve in v kakšnem obsegu lahko uporablja,
- postopki za avtorizacijo, kdo sme spreminjati dostop do določenih storitev,
- nadzorni postopki in kontrole, ki ščitijo dostop do določenih storitev.

Postopek dodelitve, spreminjanja ali odvzema uporabniških pravic je lahko voden ročno (telefon, e-pošta, pisni zahtevek) ali z uporabo sistemov (programske opreme) za upravljanje identitet. Slednji omogočajo nadzor uporabnikov z osrednjega mesta po samodejnih in vnaprej pripravljenih postopkih in pravilih. V vsakem primeru se dostopna pravica uporabniku ali skupini uporabnikov lahko dodeli na podlagi zahtevka, ki naj vsebuje najmanj:

- datum zahtevka za dodelitev ali odvzem dostopne pravice,
- podatke o predlagatelju zahtevka (npr. vodja notranje organizacijske enote, projektni vodja),
- upravičenost zahteve,
- podatke o osebi, ki ji bodo pravice dodeljene ali odvzete,
- prostor, informacijski podsistem (uporabniška rešitev) ali gradivo, do katerih bo imela (izgubila) oseba dostop,
- način (tip) dostopa oz. pravice, ki so vezane na dostop (branje, spreminjanje, brisanje itd.),
- podatke o osebi, ki je odobrila zahtevek,
- podatke o osebi, ki je zahtevek izvedla,
- datum izvedbe.

3.5. REVIZIJSKE SLEDI

Sestavni del ukrepov in postopkov za uresničevanje načel varnega zajema in e-hrambe je tudi ustvarjanje sledilnih zapisov oz. revizijskih sledi o posameznih dostopih do gradiva, o izvedenih posegih in o dostopih oz. uporabi informacijskega sistema za zajem in e-hrambo.

UVDAG[58] izrecno zahteva izdelovanje in hrambo revizijskih sledi, vezanih na zajem in pretvorbo gradiva v digitalni obliki. Ker so te sledi neposredno vezane na varovanje gradiva pred okrnjenjem njegove celovitosti, morajo biti sestavni del postopkov zajema ali pretvorbe in shranjene skupaj z gradivom.

Organizacija mora izdelovati in hraniti zapise revizijskih sledi, vezanih na dostop do hranjenega gradiva oz. reprodukcije njegove vsebine, do infrastrukture informacijskega sistema za e-hrambo in do prostorov, v katerih se hranijo nosilci zapisov gradiva oz. v katerih so nameščeni elementi informacijskega sistema.

V tem poglavju so zapisane predvsem splošne zahteve o revizijski sledi s poudarkom na načinu in roku hrambe, zahteve glede revizijskih sledi, vezanih na ISUD, pa so opredeljene v tretjem delu ETZ v poglavju Zahteve za akreditacijo programske opreme.

3.5.1 Vrste revizijskih sledi, vezanih na dostop do hranjenega gradiva

Glede *obsega revizijskih sledi* o dostopu do hranjenega gradiva ločimo tri načine beleženja revizijskih sledi:

- Prvi način omogoča naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal vsebino gradiva in kdaj. V tem primeru govorimo o beleženju t. i. *aktivnih dostopov do gradiva*.
- Drugi način omogoča beleženje, kdo in kdaj je do neke vsebine gradiva zgolj dostopal (vpogled, seznanitev), ne da bi jo spremenil (t. i. *pasivni dostopi)*.
- Pri tretjem načinu se v primeru aktivnih dostopov do gradiva beleži, kakšno je bilo stanje gradiva pred spremembo in po njej.

Pri opredeljevanju zahtevane ravni sledljivosti mora organizacija izhajati iz tveganja pri zajemu ali e-hrambi določene vrste gradiva, ki se obdeluje. Tako npr. ZVOP-1 glede obdelave občutljivih osebnih podatkov izrecno zahteva beleženje *aktivnih in pasivnih dostopov do gradiva.*

Enako velja glede določitve roka hrambe revizijskih sledi dostopanja do gradiva. Če zakoni ali na njihovi podlagi izdani predpisi ne določajo roka hrambe revizijskih sledi, organizacija praviloma upošteva petletni rok hrambe v skladu z določbami Obligacijskega zakonika, ki urejajo zastaralne roke za odškodninske terjatve za nastalo škodo.

Organizacija mora revizijske sledi hraniti tako, da so varovane pred izgubo in okrnitvijo celovitosti. Določiti mora njihovega skrbnika, osebe, pooblaščene za dostop do njihovega zapisa, ter način njihove obdelave in uporabe.

3.5.2 Revizijske sledi, vezane na dostop do opreme informacijskega sistema za e-hrambo

Organizacija mora tvoriti in shranjevati sledilne zapise oz. revizijske sledi dostopov do infrastrukture informacijskega sistema za e-hrambo in do prostorov, v katerih se hranijo nosilci zapisov gradiva oz. v katerih so nameščeni elementi informacijskega sistema.

Pri beleženju dostopov do opreme informacijskega sistema za zajem in e-hrambo mora organizacija vzpostaviti sistem hranjenja revizijskih sledi o vseh postopkih upravljanja identitet in dostopnih pravic uporabnikov infrastrukture. Obseg (kdo, kdaj, do katerega vira) in rok hrambe revizijske sledi morata temeljiti na oceni tveganja in razlogih za določitev roka hrambe revizijskih sledi dostopa do gradiva, ki se hrani na določeni infrastrukturi.

[58] UVDAG, 11., 12. in 13. člen.

Pri beleženju vstopov v prostore, v katerih je e-hranjeno gradivo oz. infrastruktura, na kateri se gradivo hrani, mora organizacija slediti določbam ZVOP-1, ki urejajo evidentiranje vstopov v prostore organizacije in izstopov iz njih (revizijska sled vstopov se mora voditi kot zbirka osebnih podatkov, njeni zapisi pa se lahko hranijo največ tri leta).

3.6. UPRAVLJANJE VARNOSTNIH INCIDENTOV

Organizacija mora predvideti ustrezne oblike odzivanja na dogodke, ki bi lahko ogrozili ali ki so že povzročili škodljive posledice za sistem zajema in e-hrambe oz. za hranjeno gradivo.

Organizacija naj v aktih o ukrepih in postopkih varovanja gradiva npr. določi:
- način evidentiranja varnostnih incidentov (sporočenih in samodejno zaznanih),
- evidenco varnostnih incidentov,
- postopke za zavarovanje in roke hrambe revizijskih sledi, ki bi bile lahko za dokaz v postopkih, vezanih na varnostni incident,
- obveznost in način poročanja zaposlenih o zaznanih varnostnih incidentih,
- način ukrepanja ob posameznem incidentu v skladu z njegovo naravo ter možnimi vplivi na varnost sistemov in gradiva v e-hrambi,
- postopek beleženja izvedenih ukrepov,
- obveznost rednega pregledovanja in analize evidentiranih varnostnih incidentov.

4. INFORMACIJSKA OPREMA IN INFRASTRUKTURA

Pod *informacijsko opremo* štejemo strojno in programsko opremo za zajem in e-hrambo, ki je tudi predmet registracijskih in akreditacijskih postopkov. Pod *informacijsko infrastrukturo* pa štejemo tudi objekte, energetsko primarno in sekundarno oz. pomožno opremo (npr. brezprekinitveni sistemi – UPS, električni generatorji), klimatske naprave ipd.

4.1. ELEKTRIČNA IN TELEKOMUNIKACIJSKA NAPELJAVA

Električni in telekomunikacijski kabli (ožičenje), po katerih se prenašajo podatki oz. ki podpirajo informacijske storitve, morajo biti zaščiteni pred možnostjo uničenja, poškodovanja ali zlorabe. Ožičenje ne sme ovirati gibanja. Za izvedbo električnih in telekomunikacijskih napeljav naj se uporablja material, ki pri gorenju ne sprošča zdravju škodljivih snovi (uporaba malodimnega oz. slabo gorljivega materiala, angl. *flame retardant*).

Ožičenje naj vedno načrtujejo in izvedejo ustrezno usposobljeni izvajalci, in sicer skladno z veljavnimi standardi in predpisi. Njegovo varnost je treba načrtovati že ob vzpostavljanju računalniških prostorov in potem pri namestitvi opreme. Pri vsaki nadgradnji ali spremembi omrežja oz. vanj vključenih naprav pa je treba varnost preveriti.

4.2. STROJNA OPREMA

V NP mora biti razvidno, katero strojno opremo za zajem, pretvorbo in dolgoročno e-hrambo organizacija uporablja (ime, proizvajalec, serija ali model).[59] UVDAG[60] določa splošne pogoje, ki jih mora izpolnjevati strojna oprema, na kateri se izvajajo zajem, e-hramba oz. spremljevalne

[59] Glej tudi ETZ 3.1.1.1 Popis informacijskih virov.

[60] ZVDAGA, 19. člen.

storitve, in sicer mora biti *skladna z mednarodnimi, državnimi* in *drugimi splošno priznanimi standardi* ter *mednarodno uveljavljena.*

Strojno opremo je treba namestiti in zavarovati tako, da bo čimbolj odpravljeno tveganje nepooblaščenega dostopa oz. poškodovanja iz okolja. Pri tem je smiselno upoštevati predvsem:

- navodila proizvajalca oz. dobavitelja opreme,
- tehnične zahteve (temperatura, vlaga, električno napajanje …),
- ergonomske zakonitosti (svetloba, telesna drža) in vpliv na druga delovna mesta.

Raven varovanja in zaščite naj bo določena glede na pomen gradiva in ocenjeno tveganje njegove izgube ali poškodovanja.

Ponudnik lahko strojno opremo tudi akreditira. Zahteve, ki jih mora izpolnjevati za pridobitev akreditacije, so opredeljene v tretjem delu ETZ 2.0 v poglavju 2. Akreditacija strojne opreme.

4.3. NOSILCI ZAPISA

V zvezi z nosilci mora organizacija skrbeti za zagotavljanje njihove uporabnosti z ustrezno opremo, hkrati pa reševati problematiko njihovega tehnološkega zastaranja in propadanja. Z NP mora določiti nosilce zapisa, ki jih uporablja za dolgoročno e-hrambo in za katere vzdržuje primerno strojno opremo ter za preverjanje katerih sistematično skrbi.

4.4. PROGRAMSKA OPREMA

4.4.1 Funkcionalni tipi programske opreme

V NP mora biti razvidno, katero programsko opremo za zajem, pretvorbo in dolgoročno e-hrambo organizacija uporablja (ime, proizvajalec, različica).[61] Programska oprema mora biti razvrščena v posamezen funkcionalni tip glede na raven uporabe, odnos med ponudnikom in stranko ter funkcionalnost. Na trgu obstajajo različni tipi programske opreme za zajem in e-hrambo, ki se razlikujejo po namenu in uporabi (funkcionalnosti). Združimo jih lahko:

- **glede na raven uporabe programske opreme:**
  - *aplikacijska programska oprema*,
  - *vmesna oprema* (angl. *middleware*),
  - *infrastrukturna programska oprema* (npr. sistem za upravljanje podatkovne zbirke);

- **glede na odnos med ponudnikom in stranko**:
  - *programska oprema po naročilu* – razvita je po naročilu za neko organizacijo, okolje oz. uporabnike,
  - *prilagojena programska oprema* – izdelana je na podlagi tržnega programa s posebnimi programskimi prilagoditvami za stranko,
  - *tržna programska oprema* – dobavljiva je v povsem enaki obliki več kakor eni stranki,
  - *po svetu razširjena tržna programska oprema* – dobavljena je v povsem enaki obliki pri več kakor 100 organizacijah v najmanj treh državah članicah EU. Zaradi razširjenosti so zahteve iz prejšnje točke poenostavljene, in sicer se v akreditacijskih postopkih ne zahteva dokumentacija o razvoju programske opreme, upravljanju njenih sprememb, specifikacij in preizkušanj;

[61] Glej tudi ETZ 3.1.1.1 Popis informacijskih virov.

- **glede na funkcionalnost**:
  - *infrastrukturna programska oprema;*
  - *programska oprema za podporo posameznim funkcionalnostim s podtipi:*
    - upravljanje gradiva v fizični obliki,
    - zajem in pretvorba izvorne analogne v digitalno obliko,
    - množični zajem (enkratno dejanje za večje sklope) in podpora e-hrambe istovrstnega gradiva (en rok hrambe, en klasifikacijski znak),
    - podpora trajne e-hrambe za gradivo, ki se ne spreminja (angl. *read only*),
    - podpora e-hrambe;
  - *programska oprema za podporo celotnemu postopku upravljanja gradiva v digitalni obliki.*

V NP morajo biti navedeni za programsko opremo vsaj naslednji podatki:

- identifikacijska oznaka oziroma ime programske opreme,
- komercialna oznaka različice programske opreme,
- vse dodatne komponente, ki sestavljajo programsko opremo in predstavljajo njeno funkcionalnost.

Dodatne komponente morajo biti, tako kot sama programska oprema, navedene z identifikacijsko oznako oziroma imenom ter komercialno oznako različice. Komercialna oznaka različice programske opreme ali komponente pomeni različico, ki se v danem trenutku trži (angl. *General availability-GA*).

4.4.2 Zahteve za programsko opremo

UVDAG[62] določa splošne pogoje, ki jih mora izpolnjevati programska oprema, na kateri se izvajajo zajem, e-hramba oz. spremljevalne storitve, in sicer mora biti *skladna z mednarodnimi, državnimi in drugimi splošno priznanimi standardi* in *mednarodno uveljavljena ali posebej razvita za organizacijo.*

Ponudnik lahko programsko opremo tudi akreditira. Zahteve, ki jih mora izpolnjevati za pridobitev akreditacije, so opredeljene v tretjem delu ETZ 2.0 v poglavju 3. Akreditacija programske opreme.

V okolju, v katerem se zahteva akreditacija (npr. varstvo arhivskega gradiva javnopravnih oseb, akreditirana storitev e-hrambe), **mora biti akreditirana programska oprema za zgoraj opisane ravni uporabe.**

4.4.3 Razvoj oz. nabava

Organizacija mora imeti sprejeto dokumentirano metodologijo razvoja programske opreme oz. postopek njene nabave. Vse zahteve za novo programsko opremo ali njeno nadgradnjo naj se predložijo nadrejenim kot specifikacija uporabniških zahtev. Merila za izbiro nove programske opreme morajo biti natančno izdelana in potrjena.

Že pri načrtovanju je treba zagotoviti združljivost programske opreme z obstoječimi sistemi v organizaciji. Če se uporablja različno programsko orodje ali njihova različica, naj organizacija določi obliko zapisa za izmenjavo in predstavitev dokumentov.

[62] ZVDAGA, 20. člen.

Že pri razvijanju programske opreme je treba izvesti analizo in specifikacijo varnostnih zahtev, ki temeljita na morebitni potrebi po zavarovanju zaupnosti, celovitosti in razpoložljivosti gradiva. Upoštevane naj bodo zahteve po:

- nadzoru dostopa do gradiva in storitev ter zaščiti pred nepooblaščenimi popravki ali spremembami,
- izdelavi revizijske sledi[63],
- preverjanju in ščitenju celovitosti ključnih podatkov,
- zaščiti zaupnih podatkov pred nepooblaščenim razkritjem (npr. šifriranje),
- upoštevanju zakonskih in pogodbenih določil,
- izdelavi rezervnih kopij in določitvi postopkov obnovitve.

Vsaka različica programske opreme (izvorna in izvršna koda) mora biti obvezno enolično označena, vse spremembe programske opreme pa se morajo dokumentirati.[64]

Za vsak preizkus programske opreme je treba izdelati natančne načrte, ki predvsem določajo, kdaj je preizkus uspel in obseg preskusnih podatkov. Preizkus je treba dokumentirati.

Okolje za razvoj in preizkušanje programske opreme mora biti ločeno od okolja za redno rabo. Preizkusno okolje naj bo kar najbolj podobno okolju za redno rabo in s stališča varnosti morajo zanj veljati enaka pravila.[65]

S preizkusnimi podatki, ki so vzeti iz okolja za redno rabo, je treba ravnati enako kakor z dejanskimi podatki. Dejanski podatki (osebni ali drugi zaupni), ki se uporabljajo v preizkusne namene, naj se popačijo (anonimizirajo).

Pred prenosom programske opreme iz preizkusnega okolja v okolje za redno rabo morajo biti v skladu z načrtom preizkusa izvedene vse kontrolne točke slednjega in potrditi jih morajo odgovorne osebe. Izdelana morata biti tudi analiza možnih vplivov uvedene različice na preostalo okolje in načrt vrnitve v prvotno, delujoče stanje. Prenos morajo odobriti pooblaščene osebe in izvedeni morajo biti postopki obveščanja o opravljenih spremembah.

Pri pripravi in sklepanju pogodbe[66] z dobaviteljem je smiselno upoštevati določbe Obligacijskega zakona[67] o licenčni pogodbi, ki v teh primerih govori o obveznostih dajalca licence, in sicer o:

- dolžnosti izročitve tehnične dokumentacije, potrebne za uporabo predmeta licence,
- dolžnosti dajanja navodil in obvestil, potrebnih za uspešno izkoriščanje predmeta licence,
- odgovornosti za tehnično izvedljivost in uporabnost predmeta licence.

[63] Glej tudi poglavje 3.5 Revizijske sledi.

[64] Glej tudi poglavje 5.1 Upravljanje sprememb.

[65] Glej tudi poglavje 5.2 Ločevanje operativnega okolja od okolja, namenjenega razvoju, in od okolja za preizkušanje.

[66] Glej tudi poglavje 6 Naročanje storitev pri zunanjem izvajalcu.

[67] Obligacijski zakonik /OZ-UPB1/ (Uradni list RS, št. 97/2007).

5. UPRAVLJANJE INFORMACIJSKE OPREME IN INFRASTRUKTURE

5.1. UPRAVLJANJE SPREMEMB

Vse spremembe informacijske opreme in infrastrukture morajo biti nadzorovane, saj lahko vplivajo na nemoteno in učinkovito izvajanje posameznih storitev. Biti morajo načrtovane, predvsem pa je treba predvideti morebitne posledice vsake spremembe.

Vzpostavljeni morajo biti ustrezni postopki za izvajanje sprememb, ki morajo biti formalizirani, nadzorovani, konsistentni med različnimi platformami in v celoti dokumentirani.

Spreminjanje in nadgrajevanje informacijske opreme in infrastrukture morata potekati najmanj v skladu s temi zahtevami:

- načrtovane spremembe morajo odobriti pooblaščene osebe,
- pred vsako spremembo morajo biti pregledane varnostne kontrole in izvedeni postopki za preverjanje pravilnosti delovanja sistema po spremembi,
- preveriti je treba, ali je zaradi spremembe potrebna dodatna prilagoditev katerega koli dela sistema (programske in strojne opreme, zbirke podatkov, datoteke …),
- vse spremembe morajo biti, preden se izvedejo v okolju za redno rabo, preverjene v preizkusnem okolju,
- vse spremembe morajo biti dokumentirane, dopolnjena mora biti dokumentacija sistema oz. njegovih sestavnih delov,
- zaradi morebitne potrebe po vrnitvi sistema v prejšnje delujoče stanje (pred spremembo) je treba pred večjo spremembo (glede na oceno tveganja) izvesti varnostno kopiranje tega stanja,
- pred posamezno spremembo, ki vpliva na delo drugih upraviteljev informacijske opreme ali infrastrukture oz. končnih uporabnikov, je treba vse vpletene obvestiti o njeni nameravani izvedbi, njenem namenu in morebitnih vplivih na njihovo delo. Obveščanje o predvidenih akcijah (spremembah), pa tudi varnostnih incidentih je lahko v pisni ali elektronski obliki (zadošča sporočilo po e-pošti).

5.2. LOČEVANJE OPERATIVNEGA OKOLJA OD OKOLJA, NAMENJENEGA RAZVOJU, IN OD OKOLJA ZA PREIZKUŠANJE

Za postopke zajema in e-hrambe je treba zagotoviti različna okolja. Navadno sta to okolje za preizkušanje (testiranje) in okolje za redno rabo (produkcijsko okolje), če organizacija tudi sama razvija programsko opremo oz. informacijski sistem, pa še razvojno okolje. V preizkusnem okolju se izvaja potrditveno preizkušanje (torej preverjanje pravilnosti delovanja informacijske rešitve v skladu z uporabniškimi zahtevami in specifikacijami) in mora biti funkcionalno ekvivalentno okolju za redno rabo. Če informacijski sistem, ki se preizkuša v preizkusnem okolju, uporablja za svoje delovanje osebne podatke oz. podatke, za katere velja omejen dostop, je treba uporabiti preizkusni izbor podatkov, iz katerih je nemogoče razbrati lastnosti ali stanja, ki bi se lahko navezala na določeno osebo. Obseg in vsebina preizkusnega izbora podatkov morata biti predhodno dogovorjena z naročnikom, lastnikom oz. upravljavcem zbirke. Uporaba neosebnih podatkov v razvojnem okolju je obvezna ne glede na lokacijo razvojnega okolja.

Po uspešnem zaključku preizkušanja pravilnosti delovanja informacijskega sistema za zajem in e-hrambo se rešitev prenese po vnaprej predpisanem in odobrenem protokolu v okolje za redno rabo – v produkcijo.

5.3. LOČEVANJE HRANJENEGA GRADIVA POSAMEZNIH ORGANIZACIJ

Ponudnik storitev mora z vpeljavo različnih nadzornih mehanizmov (fizičnih in logičnih) zagotoviti, da bo gradivo različnih strank, ki ga hrani v svojem informacijskem sistemu, strogo ločeno. Torej ima vsaka stranka lahko dostop samo do svojega gradiva, ki ga ima v e-hrambi določen ponudnik. S tem se zmanjša tveganje nepooblaščenega dostopa do gradiva druge organizacije.

5.4. ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO IN VDORI

Informacijski sistemi za zajem in e-hrambo gradiva morajo biti ustrezno zaščiteni proti virusom ter drugo škodljivo, nezaželeno in nepotrebno programsko opremo v skladu z oceno tveganja. Zaščita pred virusi in podobno zlonamerno programsko opremo se doseže z namestitvijo in uporabo ustreznega, certificiranega in registriranega protivirusnega programa, ki mora biti redno dopolnjen z zbirko virusov oz. protivirusnimi dejavnostmi.

5.5. SINHRONIZACIJA SISTEMSKIH UR

Pri medsebojni izmenjavi elektronskih dokumentov, pa tudi vseh drugih dogodkov v informacijskem sistemu (npr. vstopi v prostore, dostop do programov, izvedena sprememba na podatku) je izrednega pomena ne samo datum, ampak tudi natančen čas. Zato je treba sistemske ure informacijske opreme in infrastrukture časovno sinhronizirati z verodostojnim zunanjim časovnim virom. Primer je npr. uporaba časovnega strežnika NTP. Ta ima svoj čas sinhroniziran zelo točno, navadno z uporabo vgrajenega sprejemnika GPS, in mora biti dostopen v omrežju. Vse druge naprave, ki so priključene v omrežje (npr. strežniki, usmerjevalniki), se lahko sinhronizirajo s tem strežnikom po protokolu NTP ali SNTP. Časovni strežnik omogoča sinhronizacijo tudi drugih naprav v omrežju, kakršne so telefonske centrale, videokamere.

5.6. VZDRŽEVANJE INFORMACIJSKE OPREME IN INFRASTRUKTURE

Za doseganje želene ravni razpoložljivosti in zanesljivosti delovanja informacijske opreme in infrastrukture morata biti zagotovljena podpora in vzdrževanje. Organizacija ima lahko v ta namen sklenjene vzdrževalne pogodbe, ki naj opredelijo načine in pogoje, s posebnim poudarkom na primernem odzivnem času. V praksi velja za primeren odzivni čas začetka reševanja tisti, ki ne presega enega delovnega dne. Odzivni čas mora biti ustrezno dokazljiv (pogodba, splošni pogoji).

Pri tem je najboljši način proaktivnost, kar pomeni vnaprejšnji nadzor oz. preprečevalno vzdrževanje. Zato je vzdrževalne posege in servisiranje smiselno načrtovati. Vzdrževanje oz. servisiranje morajo opravljati zgolj usposobljeni zaposleni ali pooblaščeni izvajalci. Za načrtovanje, vzpostavitev, nadzor in vzdrževanje opreme je treba določiti odgovorno osebo. Ta mora tudi skrbeti, da bodo vsi vzdrževalni posegi ustrezno dokumentirani (npr. kdaj je bil poseg izveden, kdo ga je izvedel, kaj je napravil, razlog tega). Kadar se oprema, ki vsebuje podatke, servisira zunaj organizacije, naj se nosilci teh podatkov ali odstranijo iz naprave ali pa je treba podatke zaščititi kako drugače.

5.7. NADZOR, VARNOSTNI PREGLEDI IN ZAGOTAVLJANJE ZAPISOV O DELOVANJU SISTEMA

O delovanju informacijskega sistema in izvajanju postopkov za zajem in e-hrambo morajo obstajati ustrezni zapisi, ki dokazujejo, da sta zajem in e-hramba v skladu s postavljenimi zahtevami. Dokazujejo tudi neoporečnost hranjenega gradiva in so hkrati sami po sebi dokumentarno gradivo. Obsegajo zapise o:

- pripravi pravil in različnih postopkov (operativnih, nadzornih, preizkusnih),
- izvajanju teh postopkov,
- namestitvi in upravljanju informacijske opreme in infrastrukture.

Organizacija preverja, ali:

- je njena infrastruktura varna,
- vsi varnostni sistemi delujejo nemoteno,
- so v vmesnem času do opreme oz. podatkov vdrle ali poskušale vdreti nepooblaščene osebe.

Redno mora pregledovati in preverjati izvajanje varnostnih ukrepov in postopkov, vezanih na zajem in e-hrambo. Varnostni pregledi morajo biti opravljeni kot občasni, rutinski pregledi, pa tudi pri sumu varnostnih incidentov oz. drugih oblikah varnostnih pomanjkljivosti in biti morajo dokumentirani (obstajati morajo poročila). Ugotovitve in ukrepi, sprejeti na podlagi pregledov, morajo biti predstavljeni vodstvu organizacije, ki je odgovorno za odpravo ugotovljenih pomanjkljivosti.

Ponudniki storitev e-hrambe pa morajo skladno z UVDAG opravljati redne varnostne preglede svoje infrastrukture vsak delovni dan. Če zagotavljajo svoje storitve 24 ur na dan 365 dni na leto, pa vsak dan.

6. NAROČANJE STORITEV

6.1. POGODBENO UREJANJE NAROČANJA IZVAJANJA STORITEV (MED NAROČNIKOM IN IZVAJALCEM)

Iz različnih razlogov (npr. izboljšanje poslovanja) lahko organizacija za storitve, povezane z zajemom in e-hrambo, najame zunanjega izvajalca. Tako je gradivo dodatno izpostavljeno nevarnosti ne samo nepooblaščenega razkritja, temveč tudi izgube ali poškodovanja. Zato morata naročnik in zunanji izvajalec še pred podpisom pogodbe izdelati skupno oceno tveganja. Ta sicer ni del NP enega ali drugega, biti pa mora podlaga za sklenitev pogodbe o sodelovanju. V NP morata tako naročnik (v lastna NP) kot izvajalec storitve (v NP, ki urejajo izvajanje storitve) vključiti določbo, ki ju zavezuje k izvedbi skupne ocene tveganj s partnerjem pri izvajanju storitve in upoštevanju ugotovitev ocene tveganj pri oblikovanju določb pogodbe.

S pogodbo[68] je treba opredeliti kakovost oz. raven storitve, tako da bodo vnaprej določeni potrebni parametri za izvajanje slednje. Zato naj pogodba vključuje predvsem obseg, opis in storitvene cilje, predvideni rok trajanja oz. dobo opravljanja te storitve in obveznosti obeh pogodbenih strank. Pri opisu storitve je treba opredeliti ciljne in nesprejemljive ravni njenega izvajanja, vključno z opredelitvijo preverljivih meril za doseganje teh ravni oz. delovni učinek

[68] Pogodba, ki jo skleneta izvajalec in naročnik storitve, se navadno imenuje pogodba o zagotavljanju ravni storitve (angl. *Service Level Agreement* – SLA).

ter pravico pregleda in nadzorovanja pogodbenih obveznosti, lahko tudi s strani tretjih oseb. Izvajalca je treba s pogodbo zavezati, da bo zagotavljal poročila o delovanju storitve, ki naj se nanašajo predvsem na dogovorjene parametre slednje (npr. na skupno število incidentov ali pri e-hrambi npr. na skupni čas nedelovanja storitve). S pogodbo je treba določiti, da nesprejemljiva raven opravljanja storitve, ki se ponavlja določen čas, šteje za pogodbeno kršitev. Če bo pogodba vključevala sodelovanje s tujimi oz. mednarodnimi osebami ali organi, je treba natančno opredeliti še morebitne obveznosti glede njihove zakonodaje.

Zaradi zaupnosti podatkov, do katerih bo pri izvajanju storitev morda imel dostop zunanji izvajalec, se v pogodbo vključi določba o zaupnosti tako pridobljenih podatkov. S takim dogovorom se zunanji izvajalec storitev zaveže, da bo pridobljene podatke o organiziranosti, strojni, programski in drugi opremi, sistemih, omrežjih in druge podatke, katerih razkritje tretjim osebam bi lahko kakor koli ogrozilo ali škodovalo organizaciji, varoval kot poslovno skrivnost. Po potrebi se v pogodbo vključi še zahteva po varnostnem preverjanju oseb, zaposlenih pri izvajalcu, predvsem ko bodo ti prihajali v stik ali delali z varovanimi oz. občutljivimi podatki (npr. osebnimi podatki, podatki, ki nosijo oznako poslovna skrivnost).

V pogodbo se vključi tudi pravica organizacije do redne ali izredne revizije izvajanja storitve zunanjega izvajalca (pregled NP in njihovega izvajanja).

Kadar bo torej del postopkov, povezanih z zajemom in e-hrambo gradiva, izvajal zunanji ponudnik, se zanje uporabljajo njegova NP, za vse preostale postopke pa NP organizacije naročnice. Tako bo zagotovljeno, da bodo vsi postopki upravljanja gradiva organizacije med zajemom in e-hrambo skladni z zakonskimi in varnostnimi zahtevami, hkrati pa bo zagotovljena verodostojnost tega gradiva.

6.2. IZVAJANJE STORITEV ZA JAVNOPRAVNE OSEBE

Dodatna zahteva za javnopravne osebe, kadar najemajo storitve, povezane z zajemom in e-hrambo pri zunanjem izvajalcu, je, da je ta storitev akreditirana. Več o pogojih za pridobitev akreditacije je zapisano v tretjem delu ETZ, poglavje 4.