



Politika kvalifikovanog elektronskog čuvanja dokumenata

Verzija 1.0

OID: 1.3.6.1.4.1.16100.66100.1.1

Beograd, 15.11.2023.

Sadržaj

Uvod.....	6
1.1 Pregled	6
1.2 Naziv dokumenta i identifikacija	7
1.2.1 Usklađenost dokumenta	8
1.2.2 Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata	8
1.2.3 Stupanje na snagu	9
1.3 Učesnici	10
1.3.1 Podaci Pružaoca usluge kvalifikovanog elektronskog čuvanja dokumenata:	10
1.3.2 Pretplatnici	11
1.3.3 Pouzdajuće strane	11
1.4 Administracija dokumenta	12
1.4.1 Organizacija koja vrši administraciju dokumenta	12
1.4.2 Osoba koja je odgovorna za dokument Politika kvalifikovanog elektronskog čuvanje dokumenata	12
1.4.3. Osoba koja je odgovorna za usaglašenost dokumenta Praktična pravila kvalifikovanog elektronskog čuvanje dokumenata sa Politikom kvalifikovanog elektronskog čuvanja dokumenata	13
1.4.4. Procedura postupanja sa dokumentom Politika kvalifikovanog elektronskog čuvanja dokumenata.....	13

1.5 Skraćenice i definicije	14
1.5.1 Skraćenice	14
1.5.2 Definicije	15
2. Upravljenje repozitorijem i način objave	16
2.1 Repozitorijumi	16
2.2 Objava informacija za kvalifikovano elektronsko čuvanje dokumenata	17
3. Usluga kvalifikovanog elektronskog čuvanja	18
3.1 Zaključenje ugovora o usluzi	19
3.2 Otpremanje objekta čuvanja	19
3.3 Dostupnost i preuzimanje dokaza o čuvanju	20
3.4 Izdavanje potvrde na zahtev Pretplatnika	20
3.5 Raskid Ugovora o usluzi	21
4. Tehničke mere bezbednosti	21
4.1 Sigurnosne garancije	21
4.2 Mere predostrožnosti za računarsku bezbednost	22
4.3 Tehničke mere predostrožnosti vezane za životni ciklus	22
4.4 Kontinuirano praćenje tehnologije	22
4.5 Prihvatanje izdavaoca sertifikata i vremenskog žiga	23
4.6 Dostupnost određenih elemenata usluge elektronskog očuvanja	23
5. Kontrole objekata, upravljanja i rada	24
5.1 Fizičke kontrole	24
5.1.1 Lokacija i izgradnja	25
5.1.2 Fizički pristup	25
5.1.3 Napajanje i klimatizacija	27
5.1.4 Izloženost vodi	27
5.1.5 Prevencija i zaštita od požara	27
5.1.6 Skladištenje medija	28
5.1.7 Bekap	28
5.2 Proceduralne kontrole	28
5.2.1 Poverljive uloge	29
5.2.2 Broj potrebnih osoba po zadatku	29
5.2.3 Identifikacija i autentifikacija za svaku ulogu	29
5.2.4 Uloge koje zahtevaju razdvajanje dužnosti	30
5.3 Kontrola osoblja	30
5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje	31

5.3.2 Procedure provere	31
5.3.3 Zahtevi za obuku	31
5.3.4 Učestalost i uslovi prekvalifikacije	32
5.3.5 Učestalost i redosled rotacije poslova	32
5.3.6 Sankcije za nedozvoljene radnje	32
5.3.7 Zahtevi nezavisnog izvođača	33
5.3.8 Dokumentacija dostavljena osoblju	33
5.4 Procedure evidentiranja revizije	34
5.4.1 Vrste snimljenih događaja.....	34
5.4.2 Učestalost obrade dnevnika zapisa.....	37
5.4.3 Period zadržavanja za evidenciju revizije.....	37
5.4.4 Zaštita dnevnika zapisa	37
5.4.5 Procedure rezervne kopije dnevnika zapisa	38
5.4.6 Obaveštenje subjektu koji izaziva događaj	38
5.4.7 Procene ugroženosti	38
5.5 Arhivski zapisi	39
5.5.1 Vrste arhiviranih zapisa.....	39
5.5.2 Period čuvanja arhive.....	39
5.5.3 Zaštita arhive.....	40
5.5.4 Procedure arhiviranja rezervnih kopija.....	40
5.5.5 Zahtevi za postavljanje vremenskog žiga na zapise	40
5.5.6 Procedure za dobijanje i verifikaciju arhivskih informacija.....	41
5.6 Kompromis i oporavak od katastrofe.....	41
5.6.1 Procedure za rukovanje incidentima	41
5.6.2 Mogućnosti kontinuiteta poslovanja nakon katastrofe.....	42
5.7 Prestanak rada pružaoca kvalifikovane usluge od poverenja.....	42
6. Tehničke bezbednosne kontrole	44
6.1 Opšti zahtevi.....	44
6.2 Kontrola pristupa	44
6.2.1 Bezbednost operacija.....	45
6.3 Kontrole kompjuterske bezbednosti.....	45
6.3.1 Specifični tehnički zahtevi za bezbednost računara	45
6.3.2 Ocena računarske bezbednosti.....	46
7. Revizija usklađenosti i druge procene.....	46
7.1 Procena učestalosti	47



7.2 Identifikacija/Kvalifikacije procenjivača	48
7.3 Odnos procenitelja prema procenjenom subjektu	48
7.4 Tematski opseg procene	48
7.5 Postupci nakon otkrivanja nedostataka	49
8. Reference	50
9. Istorija rada dokumenta	53

Uvod

Ovaj dokument predstavlja Politiku pružanja kvalifikovane usluge elektronskog čuvanja dokumenata kompanije "Iron Mountain d.o.o." Novi Banovci (u daljem tekstu: "Iron Mountain d.o.o." ili Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata).

Politika kvalifikovanog elektronskog čuvanja dokumenata je u skladu sa zahtevima propisanim eIDAS Uredbom i u skladu sa zahtevima, smernicama i međunarodnim standardima, posebno ETSI SR 019 050, EN 319 401, EN 319 421, ETSI TS 119 101, ETSI EN 319 522-1, ETSI EN 319 522-2, ETSI EN 319 521 V1.1.1 (2019-02), a usluga koja se pruža u skladu sa ovim propisima je kvalifikovana za uslugu kvalifikovanog elektronskog čuvanja dokumenata.

1.1 Pregled

Politika kvalifikovanog elektronskog čuvanja dokumenata predstavlja skup osnovnih zahteva i pravila Pružaoca usluge kvalifikovanog elektronskog čuvanja dokumenata koje treba uspostaviti u vezi sa kvalifikovanim elektronskim čuvanjem dokumenata .

"Iron Mountain d.o.o." je Politici kvalifikovanog elektronskog čuvanja dokumenata dodelilo OID: 1.3.6.1.4.1.16100.66100.1.1.

Pored Politike kvalifikovanog elektronskog čuvanja dokumenata, Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata, izdaje dokument Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata koji uspostavlja operativne procedure i druga pravila i uslove u cilju ispunjenja zahteva određenih ovom Politikom i Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju.

Politika kvalifikovanog elektronskog čuvanja dokumenata i Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata su javni dokumenti.

1.2 Naziv dokumenta i identifikacija

Dokument Politika kvalifikovanog elektronskog čuvanja dokumenata se identifikuje kao što sledi:

Naziv	Vrednost
Naziv	Politika kvalifikovanog elektronskog čuvanja dokumenata
Verzija	1.0
Izdavalac	"Iron Mountain d.o.o."
OID	1.3.6.1.4.1.16100.66100.1.1
Datum stupanja na snagu	15.11.2023.
Internet adresa na kojoj je dokument objavljen	https://digidocs.rs/dokumenti/

Identifikacioni podaci Pružaoca usluge kvalifikovanog elektronskog čuvanja dokumenata dati su u nastavku:

Naziv	Vrednost
Naziv organizacije	"Iron Mountain d.o.o." Novi Banovci
Adresa organizacije	Treća Logistička 1, 22304 Novi Banovci, Srbija
Internet adresa	www.ironmountain.com

1.2.1 Usklađenost dokumenta

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata izjavljuje da je usklađen sa ETSI politikom u nastavku:

- ETSI TS 119 512
- ETSI TS 319 401

Svi ostali standardi navedeni su u dokumentu Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata u poglavlju 3. Usluga kvalifikovanog čuvanja ovog dokumenta.

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata izjavljuje da je usklađen sa Zakonom i odgovarajućim ETSI standardima kroz dokument Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata.

1.2.2 Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata

Dokument Politika kvalifikovanog elektronskog čuvanja dokumenata koji je u skladu sa Praktičnim pravilima kvalifikovanog elektronskog čuvanja dokumenata identifikuje se na sledeći način:

Naziv	Vrednost
Naziv	Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata
Verzija	1.0
Izdavalac	"Iron Mountain d.o.o."
OID	1.3.6.1.4.1.16100.66100.2.1
Datum stupanja na snagu	15.11.2023.
Internet adresa na kojoj je dokument objavljen	https://digidocs.rs/dokumenti/

1.2.3 Stupanje na snagu

Dokumenta Politika kvalifikovanog elektronskog čuvanja dokumenata i Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata, stupaju na snagu od datuma navedenom u odeljku 1.2 i treba ih revidirati prilikom svake promene u pružanju usluge, a najmanje jednom godišnje i obezbediti njihovu dopunu potencijalno izmenjenim zahtevima, uslovima i pravilima.

Obuhvatnost usluge

Politika kvalifikovanog elektronskog čuvanja dokumenata definiše specifične zahteve za usluge opisane u ovom dokumentu.

Obuhvatnost učesnika

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata pruža usluge pravnim licima registrovanim u Republici Srbiji.

Vremenski okvir

Trenutna verzija dokumenta Politika kvalifikovanog elektronskog čuvanja dokumenata je na snazi od datuma stupanja na snagu navedenog u odeljku 1.2 Naziv dokumenta i identifikacija. Dejstvo ovog dokumenta prestaje po prekidu pružanja usluge ili izdavanjem nove verzije dokumenta Politika kvalifikovanog elektronskog čuvanja dokumenata.

Geografsko pokriće

Dokument Politika kvalifikovanog elektronskog čuvanja dokumenata je u skladu sa zakonodavstvom Republike Srbije i prema zahtevima Evropske unije.

Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata može proširiti geografski opseg svoje usluge, pri čemu neće koristiti manje rigorozne zahteve od onih propisanih u dokumentima Politika kvalifikovanog elektronskog čuvanja dokumenata i Praktična pravila za kvalifikovano elektronsko čuvanje dokumenata.

Usluga koja se pruža u skladu sa ovim dokumentom Politika kvalifikovanog elektronskog čuvanja dokumenata dostupna je globalno.

Usluga koja se pruža u skladu sa dokumentom Politika kvalifikovanog elektronskog čuvanja dokumenata može se koristiti samo kako je opisano u ovom dokumentu, kao i u dokumentu Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata.

Politika kvalifikovanog čuvanja elektronskih dokumenata je identifikovana formalnim registrovanim identifikatorom objekta (OID) 1.3.6.1.4.1.16100.66100.1.1.

“Iron Mountain d.o.o.” će navedeni OID koristiti u izveštajima koje izdaje korisnicima.

1.3 Učesnici

1.3.1 Podaci Pružaoca usluge kvalifikovanog elektronskog čuvanja dokumenata:

Naziv: “Iron Mountain d.o.o.” Novi Banovci
Sedište: Novi Banovci
Telefon: +381 (0) 11 3239336
Internet adresa: www.ironmountain.com

“Iron Mountain d.o.o.” Novi Banovci je deo globalne kompanije Iron Mountain Inc. koja se bavi pružanjem usluge upravljanja dokumentima i informacijama i pružalac je kvalifikovane usluga od poverenja “Kvalifikovano elektronsko čuvanje dokumenata”. U svom radu koristi maksimalne nivoe obezbeđenja i sigurnosti podataka kako prilikom prenosa tako i prilikom čuvanja istih.

Uslugu izdavanja kvalifikovanih sertifikata za elektronski potpis/pečat, validacije kvalifikovanog elektronskog potpisa, kao i uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova koristi putem dobavljača - *Privredne komore Srbije*, pružaoca kvalifikovanih usluga od poverenja akreditovanog od strane nadležne institucije Republike Srbije.

Za potrebe pružanja usluge kvalifikovanog elektronskog čuvanja dokumenata, Iron Mountain doo iznajmljuje računarske resurse na platformi *Data Cloud Technology doo, Kragujevac*.

U pogledu razvoja softvera, integracije sistema i informacionih tehnologija, Iron Mountain doo koristi usluge partnera *Enetel Solutions doo Beograd*.

Pružalac usluge nudi pouzdane usluge u skladu sa važećim pravnim aktima Republike Srbije i Evropske unije, a posebno u skladu sa eIDAS Uredbom[1] i u skladu sa tehničkim zahtevima,

smernicama i međunarodnim standardima, posebno ETSI SR 019 050, EN 319 401, EN 319 421 , ETSI TS 119 101, ETSI EN 319 522-1, ETSI EN 319 522-2, ETSI EN 319 521 V1.1.1 (2019-02). Pružalac usluge planira i primenjuje sve mere zaštite u skladu sa standardima ISO/IEC 27001 i ETSI tehničkim zahtevima.

Kvalitet i informaciona bezbednost

Pružalac usluge planira i primenjuje sve mere zaštite u skladu sa standardima ISO/IEC 27001i ETSI tehničkim zahtevima.

1.3.2 Pretplatnici

Pretplatnici (klijenti) definišu prava i obim korisnika koji koriste uslugu i pokrivaju naknade koje se odnose na korišćenje ove usluge. Pretplatnici su pravna lica koja sa "Iron Mountain d.o.o". zaključe Ugovor o korišćenju usluge kvalifikovanog čuvanja elektronskih dokumenata.

1.3.3 Pouzdajuće strane

Pouzdujuće strane su pravna lica koja se pouzdaju u uslugu kvalifikovanog čuvanja elektronskih dokumenata. Pre pouzdanja u uslugu, pouzdajuće strane moraju da realizuju procedure provere predmetne usluge definisane dokumentom Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata.

1.4 Administracija dokumenta

1.4.1 Organizacija koja vrši administraciju dokumenta

Podaci organizacije koja administrira ovaj dokument dati su u nastavku:

Naziv	Vrednost
Naziv organizacije	"Iron Mountain d.o.o." Novi Banovci
Adresa organizacije	Treća Logistička 1, 22304 Novi Banovci
Telefon	011/3239336
Email adresa	office_rs@emea.ironmountain.com

1.4.2 Osoba koja je odgovorna za dokument Politika kvalifikovanog elektronskog čuvanje dokumenata

Naziv	Vrednost
Odgovorno lice	Benil Misini
Naziv organizacije	"Iron Mountain d.o.o." Novi Banovci
Adresa organizacije	Treća Logistička 1, 22304 Novi Banovci
Telefon	011/3239336
Email adresa	benil.misini@emea.ironmountain.com

1.4.3. Osoba koja je odgovorna za usaglašenost dokumenta Praktična pravila kvalifikovanog elektronskog čuvanje dokumenata sa Politikom kvalifikovanog elektronskog čuvanja dokumenata

Naziv	Vrednost
Odgovorno lice	Benil Misini
Naziv organizacije	"Iron Mountain d.o.o." Novi Banovci
Adresa organizacije	Treća Logistička 1, 22304 Novi Banovci
Telefon	011 / 3239336
Email adresa	benil.misini@emea.ironmountain.com

1.4.4. Procedura postupanja sa dokumentom Politika kvalifikovanog elektronskog čuvanja dokumenata

"Iron Mountain d.o.o." ima odgovornost za izradu i upravljanje dokumentom Politika kvalifikovanog elektronskog čuvanja dokumenata, uključujući redovnu reviziju i ažuriranje.

Politika kvalifikovanog elektronskog čuvanja dokumenta je javno dostupna na internet adresi: <https://digidocs.rs/dokumenti/>.

Ovaj dokument ostaje na snazi sve do stupanja na snagu nove Politike kvalifikovanog elektronskog čuvanja dokumenata ili objavljivanja prestanka njegove važnosti. Od dana stupanja na snagu nove verzije primenjuju se odredbe iz tog dokumenta na uslugu od poverenja definisanu u njemu. "Iron Mountain d.o.o." svojim internim pravilima definiše vremenski interval kontrole ovog dokumenta, odnosno periodično kontroliše i po potrebi ažurira dokument.

Politika kvalifikovanog elektronskog čuvanja dokumenata i pružanje usluge nadgleda Ministarstvo informisanja i telekomunikacija. Ministarstvo vodi Registar sa politikama usluga i Pružaocima usluga čuvanja koji primenjuju ove politike.

1.5 Skraćenice i definicije

1.5.1 Skraćenice

U okviru dokumenta Politika kvalifikovanog elektronskog čuvanja dokumenata uvode se sledeće skraćenice:

Skraćenica	Opis
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
LTA	Long Term Availability
PKSCA	Sertifikaciono telo Privredne komore Srbije
ETSI	European Telecommunications Standards Institute
XML	Extensible Markup Language
OID	Indentifikator dokumenta
MIT	Ministarstvo informisanja i telekomunikacija Republike Srbije
LDAP	Lightweigh Directory Access Protocol
SLA	Service Level Agreement
UPS	Jedinica za neprekidno napajanje
VPN	Virtual Private Network
IKT	Informaciono Komunikacione Tehnologije
TCP	Transmission Control Protocol
DMS	Document Management System
UTC	Coordinated Universal Time
eIDAS	Electronic Identification, Authentication and Trust Services
UPS	Uninterruptible Power Supply
SSL/TLS	Secure Sockets Layer or Transport Layer Security

1.5.2 Definicije

U okviru dokumenta Politika kvalifikovanog elektronskog čuvanja dokumenata uvode se sledeće definicije:

Definicija	Opis
e-dokument	Elektronski dokument koji sadrži najmanje jedan elektronski potpis ili pečat u skladu sa eIDAS Uredbom.
Status validacije	Krajnji rezultat validacije koji je dostupan Pretplatniku
Izveštaj validacije	Izveštaj koji se isporučuje Pretplatniku da bi se omogućio uvid u razloge iz kojih je proizišao odgovarajući status validacije
Usluga čuvanja	Usluga od poverenja kvalifikovanog elektronskog čuvanja koja može da produži status važenja elektronskog potpisa/pečata na duži vremenski period i da pruži dokaze o postojanju podataka tokom dužeg vremenskog perioda; odnosno usluga čuvanja je usluga kvalifikovanog elektronskog čuvanja dokumenata
Klijent	Označava pravna lica koja potpisuju ugovor o usluzi sa Pružaocem usluge čuvanja da bi koristili ugovorno opisane usluge
Korisnik	Pretplatnik i svako lice kome Klijent daje korisnička prava u okviru pretplatničkog okruženja
Administrator	Korisnik kod Klijenta koji ima nalog administratora u okviru izolovanog pretplatničkog okruženja.
Data Centar	Fizički objekat ili prostor u kojem se čuvaju, procesuiraju i upravljaju podacima. To je centralizovani skup računarskih resursa, uključujući servere, skladišta podataka, mrežnu opremu i pripadajuću infrastrukturu, koji se koriste za čuvanje, obradu, analizu i distribuciju podataka.
Skladišni prostor	Izolovani skladišni prostor koji Klijentu stoji na raspolaganju u okviru usluge čuvanja
Elektronski vremenski žig	Skup podataka u elektronskom obliku koji druge podatke u elektronskom obliku vezuje za određeno vreme čime se utvrđuje dokaz da su poslednji podaci postojali u to vreme
Elektronski potpis	Skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (potpisanim) podacima u elektronskim obliku tako da se elektronskim potpisom potvrđuje integritet tih podataka i identitet potpisnika
Elektronski pečat	Skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (pečatiranim) podacima u elektronskom

	obliku tako da se elektronskim pečatom potvrđuje integritet tih podataka i identitet pečatioca
Pretplatnik	Označava pravna lica koja potpisuju ugovor o usluzi sa Pružaocem usluge čuvanja da bi koristili ugovorno opisane usluge
Ugovor o usluzi	Ugovor između pružaoca usluge od poverenja i klijenta usluge od poverenja, koji obuhvata uslove za pružanje usluge od poverenja i za korišćenje usluge
Kvalifikovana usluga od poverenja	Usluga od poverenja koja ispunjava primenjive zahteve propisane eIDAS uredbom
Pružalac usluge čuvanja	Pružalac usluge kvalifikovanog elektronskog čuvanja dokumenata

2. Upravljenje repozitorijem i način objave

2.1 Repozitorijumi

"Iron Mountain d.o.o." je odgovoran za objave i informacije koje se odnose na ugovorne uslove i politiku pružanja usluge kvalifikovanog elektronskog čuvanja dokumenata.

Objave ugovornih uslova, obrazac ugovora i politika nalaze se na sledećoj internet stranici: <https://digidocs.rs/dokumenti/>.

Verzija novih dokumenata koja se uvodi, biće objavljena na internet stranici <https://digidocs.rs/dokumenti/>, 30 (trideset) dana pre stupanja na snagu.

Klijentu će nakon zaključenja ugovora biti dostupno na trajnom mediumu ili na načinu na koji može biti preuzeto od strane klijenta sledeća dokumenta:

- Opšti uslovi
- Ugovor o usluzi
- Politika kvalifikovanog elektronskog čuvanja dokumenata
- Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata
- Izjava o otkrivanju podataka (Disclosure Statement)

"Iron Mountain d.o.o." može pružiti Klijentu pojedinačni Ugovor o usluzi na dva različita načina:

- Na papiru, overen svojeručnim potpisom i pečatom
- U elektronskom formatu u PDF obliku sa kvalifikovanim elektronskim potpisom

"Iron Mountain d.o.o." blagovremeno obaveštava svoje Klijente o promeni Opštih uslova pisanim putem na zvaničan mejl koji je naveden u Ugovoru o pružanju usluge.

2.2 Objava informacija za kvalifikovano elektronsko čuvanje dokumenata

Osnovni uslovi za pružanje usluga navedeni su u Ugovoru o uslugama koji Klijent potpisuje prilikom zaključenja ugovora ili u pratećem dokumentu Opšti uslovi na koje se ugovor poziva.

Ažurirana Politika kvalifikovanog elektronskog čuvanja dokumenata, nakon odobrenja, objavljuju se na internet stranici <https://digidocs.rs/dokumenti/>.

Svakom izmenjenom dokumentu dodeljuje se novi broj verzije sa svakom izmenom, bez obzira na složenost promene. Prihvaćeni dokument biće poslat na uvid Ministarstvu informisanja i telekomunikacije, 30 dana pre planiranog stupanja na snagu.

"Iron Mountain d.o.o." vrši reviziju Opštih uslova jednom godišnje ili ranije u slučaju vanrednog zahteva za promenu sa prioriteto i vrši neophodne izmene.

3. Usluga kvalifikovanog elektronskog čuvanja

Primarni zadatak usluge dugoročnog čuvanja je čuvanje validnosti kvalifikovanog elektronskog potpisa/pečata na elektronskim dokumentima redovnim ažuriranjem uskladištenih kvalifikovanih elektronskih potpisa/pečata. Prilikom produženja važenja, na kvalifikovani elektronski potpis/pečat stavlja se arhivski vremenski žig, koji obezbeđuje da se validnost zadržanog originalnog kvalifikovanog elektronskog potpisa/pečata može proveriti još određeni vremenski period.

S obzirom da politika kvalifikovanog elektronskog čuvanja dokumenata ima za cilj da definiše uslove za dugoročnu garanciju validnosti kvalifikovanih elektronskih potpisa/pečata, nije moguće prihvatanje i čuvanje objekata bez kvalifikovanog elektronskog potpisa/pečata. U okviru dokumenta Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata, Pružalac usluge je specificirao prihvaćene formate elektronskih potpisa i pečata i sve druge potrebne parametre koji određuju obim usluge čuvanja.

U okviru usluge kvalifikovanog elektronskog čuvanja dokumenata mora se obezbediti sledeće:

- Pretplatnik može da otpremi elektronski dokument koji sadrži najmanje jedan elektronski potpis ili pečat u arhivu kojom upravlja Pružalac usluge čuvanja. Na osnovu heš vrednosti dokumenta, Pružalac usluge čuvanja proverava validnost elektronskih potpisa/pečata odgovarajućeg dokumenta, dopunjava ili sastavlja dokaze o čuvanju, stavlja kvalifikovani vremenski žig za elektronsku arhivu na dokaz o čuvanju, i čuva dokument i metapodatke prihvaćenog elektronskog dokumenta kao objekta za čuvanje.
- Pružalac usluga čuvanja na bezbedan način čuva objekte čuvanja, obezbeđuje da tokom celog perioda čuvanja samo ovlašćena lica imaju pristup sačuvanim podacima i da ovlašćeni Pretplatnik ima kontinuirani pristup sačuvanim podacima.
- Pružalac usluge čuvanja obezbeđuje dugoročnu validnost elektronskih potpisa i pečata postavljenih na elektronskim dokumentima. Pružalac usluge čuvanja obezbeđuje dugoročnu čitljivost objekata čuvanja tokom perioda čuvanja.
- Pretplatnik ima kontinuiran pristup objektima čuvanja i odgovarajućim dokazima o čuvanju.

- Na zahtev Pretplatnika, Pružalac usluge može da izda autentičnu potvrdu da čuva objekat čuvanja, odnosno da su u trenutku pripreme za elektronsku arhivu bili važeći elektronski potpisi ili pečati iz elektronskog dokumenta.

3.1 Zaključenje ugovora o usluzi

Pre korišćenja usluge, Pretplatnik mora da zaključi ugovor o usluzi sa Pružaocem usluge čuvanja.

Dokument Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata obezbeđuje korisnicima dovoljno informacija na osnovu kojih se mogu upoznati sa obimom usluge i odlučiti o prihvatanju usluge.

3.2 Otpremanje objekta čuvanja

Preduslov za otpremanje objekata jeste jednoznačna identifikacija Pretplatnika, odnosno Pretplatnik mora da prođe proces autentifikacije i autorizacije za rad na sistemu.

Otpremanje elektronskog dokumenta se odvija preko zaštićene SSL/TLS veze korišćenjem interfejsa koji obezbeđuje Pružalac usluge čuvanja.

Pružalac usluge čuvanja proverava usklađenost i validnost elektronskog dokumenta (odnosno proverava validnost kvalifikovanih elektronskih potpisa/pečata).

Pružalac usluge čuvanja u najkraćem roku, a ne duže od 3 dana, šalje obaveštenje Pretplatniku o rezultatima validacije i da li je zahtev za čuvanje prihvaćen ili odbijen.

U slučaju da je zahtev za čuvanje prihvaćen, generišu se dokazi o čuvanju koji su nadalje dostupni Pretplatniku u skladu sa dodeljenim ovlašćenima.

Pružalac usluge čuvanja odgovoran je za obezbeđivanje dugoročne verodostojnosti uključenih kvalifikovanih elektronskih potpisa i pečata u slučaju slanja pozitivne potvrde Pretplatniku, pa se uspešna potvrda prihvatanja objekta čuvanja nadalje potvrđuje kvalifikovanim elektronskim

pečatom i kvalifikovanim elektronskim vremenskim žigom. Konverzijom u LTA format, odnosno dodavanjem arhivskog vremenskog žiga, elektronski dokument je spreman za arhiviranje.

3.3 Dostupnost i preuzimanje dokaza o čuvanju

Pružalac usluge čuvanja obezbeđuje da Pretplatnik sa odgovarajućim ovlašćenjima može da preuzme odgovarajući dokaz o čuvanju tokom perioda važenja Ugovora o usluzi.

Pretplatnik ima pristup, putem bezbednog kanala, samo dokazima o čuvanju kojima ima pravo da pristupi u okviru izolovanog pretplatničkog okruženja koje mu je dodeljeno.

Preuzimanje dokaza o čuvanju od strane Pretplatnika vrši se putem zaštićene SSL/TLS veze.

3.4 Izdavanje potvrde na zahtev Pretplatnika

Na zahtev Pretplatnika, Pružalac usluge čuvanja izdaje potvrdu u vezi sa elektronskim dokumentom koji je otpremljen na čuvanje a koja sadrži minimalno sledeće elemente: naziv i identifikator Pretplatnika, datum i vreme prijema objekta čuvanja u arhivu, izjavu da kvalifikovani elektronski potpisi/pečati/vremenski žigovi i odgovarajući sertifikati bili važeći u vreme vremenskog žigosanja i validacije nakon njihovog otpremanja; heš dokumenta, jedinstveni identifikator dokumenta, itd. Odnosno, potvrda mora da sadrži sve potrebne i dovoljne informacije koje potvrđuju validnost u određenom vremenskom trenutku.

Izdavanje potvrde može zahtevati ovlašćeni predstavnik Pretplatnika ako i samo ako je prethodno predočio ovlašćenje Pretplatnika u dokumentu koji sadrži i njegov potpis.

Pružalac usluge čuvanja izdaje papirnu potvrdu ili elektronsku potvrdu sa kvalifikovanim elektronskim potpisom/pečatom. Potvrdu kreira odgovorno lice kod Pružaoca usluge koje je odgovorno za izdavanje arhivske potvrde.

3.5 Raskid Ugovora o usluzi

Pružalac usluge čuvanja obezbeđuje Pretplatniku pristup dokazima o čuvanju podataka tokom 60 (šezdeset) dana nakon završetka Ugovora o usluzi. U tom periodu, Pretplatnik ima mogućnost samo preuzimanja podataka, sa ograničenim pristupom drugim funkcijama u okviru pretplatničkog okruženja. Nakon isteka ovog roka, Pretplatnik neće moći pristupiti svom pretplatničkom okruženju, a samim tim ni objektima čuvanja i dokazima o čuvanju.

4. Tehničke mere bezbednosti

4.1 Sigurnosne garancije

Pružalac usluga čuvanja koristi pouzdane sisteme i proizvode zaštićene od modifikacija. Za pružanje svojih usluga koristi jedinstven IT sistem koji se sastoji od pouzdanih, tehnički procenjenih i sertifikovanih bezbednosnih proizvoda. Pružalac usluga čuvanja koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija.

Pružalac usluga čuvanja čuva arhivirane objekte zaštite u fizički zaštićenom okruženju, u skladu sa fizičkim i proceduralnim zahtevima opisanim u odeljku 6, čiju bezbednost garantuju politike unutrašnje bezbednosti i redovne unutrašnje i eksterne bezbednosne revizije. Pružalac usluge čuvanja dostavlja dokaze o čuvanju trećoj strani (npr. nadležnom organu) samo ako to Pretplatnik ovlasti ili kada je to zakonom propisano.

Integritet skladištenih podataka obezbeđen je fizičkom zaštitom i arhitekturom sistema, kao i tehnologijama vezanim za elektronske potpise. Dostupnost evidencije o čuvanju obezbeđena je

kvalitetnim sistemom Pružaoca usluge čuvanja i internim propisima koji regulišu sistem, procedurama za kontinuitet poslovanja i upravljanjem vanrednim situacijama i drugim procedurama za upravljanje vanrednim situacijama. Pružalac usluga čuvanja čuva arhivirane objekte zaštite na 2(dve) infrastrukturne instance. Pružalac usluge čuvanja uništava arhivirane objekte čuvanja na zahtev pretplatnika.

4.2 Mere predostrožnosti za računarsku bezbednost

Kada je reč o pružanju usluga čuvanja, koristimo pouzdane IT sisteme i tehnološka rešenja. Svi sistemi su redundantni kako bismo osigurali pouzdanost. Sve ključne komponente našeg sistema rade kroz dve instance, i u slučaju da jedna od njih prestane da bude operativna, druga odmah preuzima operaciju.

4.3 Tehničke mere predostrožnosti vezane za životni ciklus

Da bi se ispunio visok nivo bezbednosnih zahteva u svim projektima razvoja sistema Pružaoca usluga čuvanja, povišeni zahtevi će se uzeti u obzir u celokupnom procesu razvoja (čak i u fazi planiranja i definisanja zahteva).

Proizvodi koji se koriste za pružanje usluge čuvanja primenjuju se uzimajući u obzir bezbednosna pitanja vezana za životni ciklus.

4.4 Kontinuirano praćenje tehnologije

Pružalac usluga čuvanja, u saradnji sa PKSCA kao nadležnim organom za kvalifikovano vremensko žigosanje, kreiranje i validaciju kvalifikovanih elektronskih potpisa/pečata, kontinuirano prati razvoj tehnologije u vezi sa elektronskim potpisom i kriptografijom. Ukoliko Pružalac usluge čuvanja sazna da kriptografski algoritam sa datim parametrom koji prihvata nadležno ministarstvo u Srbiji više nije bezbedan, o tome obaveštava nadležno ministarstvo u Srbiji i zahteva reviziju odluke koja se odnosi na kriptografske algoritme.

Takođe, Pružalac usluge čuvanja kontinuirano prati razvoj tehnologije u okviru celokupnog IT rešenja, vodeći računa da sistemske komponente softvera i biblioteke imaju ažurne verzije, sa ciljem da se eliminišu sve potencijalne bezbednosne pretnje usled eventualnih sigurnosnih propusta u korišćenju biblioteka.

4.5 Prihvatanje izdavaoca sertifikata i vremenskog žiga

Pružalac usluge čuvanja koristi usluge drugog pružaoca usluge od poverenja: na sledeće načine tokom pružanja usluge:

- Usluga kvalifikovanog vremenskog žigosanja od Privredne komore Srbije
- Usluga kvalifikovane validacije od Privredne komore Srbije
- Uslugu kvalifikovanog elektronskog pečata od Privredne komore Srbije

4.6 Dostupnost određenih elemenata usluge elektronskog očuvanja

Godišnja dostupnost usluge dugoročnog čuvanja je 99,4%, a povremeni prekidi usluge ne smeju biti duži od ukupno 2 dana.

Radno vreme korisničke službe Pružaoca usluga čuvanja je od 08h do 17h.

Služba za korisnike Pružaoca usluga čuvanja prihvata zahteve za izdavanje potvrde svakog radnog dana tokom radnog vremena; izdavanje potvrde se odvija u vremenskom roku od najviše 3(tri) dana.

Pružalac usluge čuvanja ima pravo da suspenduje uslugu otpremanja elektronskih dokumenta na čuvanje, uz mogućnost uvida u već otpremljenih dokumenata i generisanih dokaza čuvanja.

5. Kontrole objekata, upravljanja i rada

Pružalac usluga čuvanja primenjuje fizičke, proceduralne i mere bezbednosti osoblja koje su u skladu sa priznatim standardima, zajedno sa administrativnim i upravnim procedurama koje ih primenjuju. Pružalac usluge čuvanja koristi zaštitne mere proporcionalne rizicima u vezi sa pojedinačnim elementima.

Pružalac usluge čuvanja prati zahteve za kapacitetom i osigurava da su adekvatna procesorska snaga i skladištenje dostupni za pružanje usluge čuvanja.

5.1 Fizičke kontrole

Pružalac usluga čuvanja vodi računa da fizički pristup kritičnim uslugama bude kontrolisan i da fizički rizik imovine koja se odnosi na kritične usluge drži na minimumu. Svrha fizičkih mera predostrožnosti je sprečavanje nezakonitog pristupa, oštećenja i neovlašćenog pristupa informacijama i fizičkim zonama Pružaoca usluge čuvanja. "Iron Mountain d.o.o." ovo reguliše procedurom "P-014 Kontrola pristupa resursima".

Usluge koje obrađuju kritične i osetljive informacije implementira se na bezbednoj lokaciji u sistemu Pružaoca usluga čuvanja.

Da bi obezbedio adekvatnu sigurnost:

- Pružalac usluga čuvanja primenjuje visoko zaštićene usluge na lokaciji Dražavnog Data centra. Ovi data centri su specijalno dizajnirani i izgrađeni kako bi zadovoljili specifične potrebe, obezbeđujući ujednačenu implementaciju različitih aspekata bezbednosti. To uključuje pozicioniranje i strukturu lokacije, kontrolu fizičkog pristupa (kroz kontrolu pristupa i nadzor), osiguranje napajanja, klimatizaciju, zaštitu od curenja vode i poplava, prevenciju i zaštitu od požara, kao i bezbedno skladištenje medija i drugih elemenata.
- Pružalac usluge čuvanja implementira svaku kritičnu uslugu i svaki neophodan alat u zasebnoj bezbednosnoj zoni.

Opšti uslovi Data centra od 1.6.2021. godine, primenjeni na ugovorni odnos između "Iron Mountain d.o.o." i Data Cloud Technologies, jasno propisuju obaveze u vezi sa čuvanjem poverljivosti podataka, zaštitom ličnih podataka, uslovima prihvatljivog korišćenja, kao i pružanjem usluga u skladu sa nivoom usklađenosti (SLA), čime se uspostavlja temeljna osnova za sistematsko i efikasno sprovođenje fizičke sigurnosti u Data centru.

5.1.1 Lokacija i izgradnja

IT sistem Pružaoca usluga čuvanja je implementiran u Državnom Data centru sa fizičkom i logičkom zaštitom koja sprečava nelegitiman pristup.

Odbrambena rešenja – kao što su na primer zaštita, sigurnosne brave, sistemi za detekciju upada, sistem video nadzora, sistem kontrole pristupa – primenjuju se tokom lociranja i uspostavljanja Data centra koji su međusobno izgrađeni i međusobno zavisni i zajedno pružaju moćnu zaštitu. sistem za IT sisteme koji učestvuju u pružanju usluga i za očuvanje poverljivih podataka koje čuva Pružalac usluga čuvanja.

Opšti uslovi Data centra od 1.6.2021. godine, primenjeni na ugovorni odnos između "Iron Mountain d.o.o." i Data Cloud Technologies, jasno propisuju obaveze u vezi sa čuvanjem poverljivosti podataka, zaštitom ličnih podataka, uslovima prihvatljivog korišćenja, kao i pružanjem usluga u skladu sa nivoom usklađenosti (SLA), čime se uspostavlja temeljna osnova za sistematsko i efikasno sprovođenje fizičke sigurnosti u Data centru.

5.1.2 Fizički pristup

Pružalac usluge čuvanja štiti uređaje i opremu koji učestvuju u pružanju usluge od neovlašćenog fizičkog pristupa kako bi sprečio neovlašćeno korišćenje uređaja.

Pružalac usluga čuvanja obezbeđuje da:

- svaki ulazak u Data centre bude registrovan

- ulazak u Data centre može se desiti samo nakon istovremene identifikacije dva ovlašćena člana osoblja sa pouzdanim ulogama – a najmanje jedan od članova osoblja treba da bude administrator sistema
- lica bez nezavisnog ovlašćenja mogu boraviti u Data centru samo u opravdanim slučajevima, potrebno vreme i u pratnji osoblja sa odgovarajućim pravima
- se dnevnicima unosa kontinuirano arhiviraju i evaluiraju

Aktivacioni podaci (lozinke, PIN kodovi) uređaja ne smeju se otvoreno čuvati čak ni u Data centru. U prisustvu neovlašćenih lica:

- mediji sa podacima koji sadrže osetljive informacije su fizički van domašaja
- prijavljeni terminali ne ostaju bez nadzora
- ne sprovodi se radni proces tokom kojeg se mogu otkriti poverljive informacije

Prilikom napuštanja računarske sobe administrator će proveriti da:

- nema terminala koji je ostao prijavljen
- alarmni sistem je aktiviran
- fizički uređaji za skladištenje su pravilno zaključani
- sistemi i uređaji koji obezbeđuju fizičku zaštitu rade ispravno
- celokupna oprema Data centra je u adekvatno bezbednom radnom stanju

Opšti uslovi Data centra od 1.6.2021. godine, primenjeni na ugovorni odnos između "Iron Mountain d.o.o." i Data Cloud Technologies, jasno propisuju obaveze u vezi sa čuvanjem poverljivosti podataka, zaštitom ličnih podataka, uslovima prihvatljivog korišćenja, kao i pružanjem usluga u skladu sa nivoom usklađenosti (SLA), čime se uspostavlja temeljna osnova za sistematsko i efikasno sprovođenje fizičke sigurnosti u Data centru.

5.1.3 Napajanje i klimatizacija

Pružalac usluge čuvanja je obezbedio da njihovi provajderi Data centra imaju jedinice za neprekidno napajanje (UPS) i rezervne generatore koji:

- imaju adekvatan kapacitet da obezbede napajanje za svoje objekte i sisteme,
- štiti IT opremu od promene napona u spoljnoj mreži, nestanka struje, skokova i drugog
- u slučaju dugotrajnog nestanka struje imaju dovoljno kapaciteta i mogućnosti dopunjavanja goriva da pokreće generatore u bilo kom vremenskom periodu.

5.1.4 Izloženost vodi

Adekvatna zaštita od prodora vode i poplava obezbeđena je za opremu u Data centrima Pružaoca usluga čuvanja.

5.1.5 Prevencija i zaštita od požara

Provajderi u Data centru Pružaoca usluga čuvanja imaju sisteme za zaštitu od požara odobrene od nadležnih organa. Detektori dima i požara automatski upozoravaju vatrogasnu brigadu. Na jasno vidljivim mestima u svakoj prostoriji nalazi se vrsta i količina ručnih aparata za gašenje požara u skladu sa važećim propisima.

Svi zaposleni ispunjavaju zakonsku obavezu o godišnjoj protivpožarnoj obuci i proveru znanja, uz odgovarajuće izveštaje.

5.1.6 Skladištenje medija

Pružalac usluga čuvanja štiti svoja skladišne medijume od neovlašćenog pristupa i slučajnog oštećenja. Svi podaci se čuvaju u rezervnoj kopiji na drugoj infrastrukturnoj instanci kao što je opisano u poglavlju 5.5.4 procedura arhiviranja rezervnih kopija.

Skladišteni mediji su zaštićeni od štetnih uticaja okoline kao što su niske ili visoke temperature, prljavština, vlaga, sunčeva svetlost, jaka magnetna polja, jako zračenje.

5.1.7 Bekap

Pružalac usluge čuvanja svakog dana kreira rezervne kopije iz kojih bi se cela usluga mogla vratiti u slučaju fatalne greške.

Rezervne kopije – barem uključujući poslednju potpunu rezervnu kopiju – čuvaju se na identičnim infrastrukturnim instancama u Data centru sa istom fizičkom i operativnom zaštitom. Bezbedan prenos podataka između infrastrukturnih instanci uspostavlja se preko lokalne mreže i odgovarajućih softverskih alata.

5.2 Proceduralne kontrole

Proceduralne mere predostrožnosti su namenjene ne samo kao dopuna, već i kao pojačanje efikasnosti fizičkih mera zaštite. To postizemo sprovođenjem dodatnih koraka usmerenih na osoblje, uključujući imenovanje i izolaciju pouzdanih uloga, jasno dokumentovanje odgovornosti svake uloge, precizno određivanje broja zaposlenih i isključujućih uloga prilagođenih različitim zadacima. Dodatno, uspostavljanjem standarda za identifikaciju i autentifikaciju unutar različitih uloga, obezbeđujemo doslednost i sigurnost u svim operativnim aspektima. Pojedinci odgovorni za određeni sistemski element ili proces jasno su dodeljeni svakom pojedinom delu sistema, eliminisanjem svake nedoumice u vezi sa odgovornostima unutar sistema. Zadaci povezani sa razvojem i operacijama su oštro razdvojeni u okviru sistema pružaoca usluga čuvanja.

5.2.1 Poverljive uloge

Pružalac usluga očuvanja definiše sledeće pouzdane uloge, sa sledećim odgovornostima:

- Menadžer Implementacije
- Inženjer baza podataka
- Sistem inženjer
- Službenik obezbeđenja
- Inženjer za podršku
- Administrativni radnik
- Pravni savetnik
- Interni revizor

Detaljne odgovornosti uloga od poverenja opisane se u dokumentu Praktična pravila kvalifikovanog elektronskog čuvanja dokumenata.

5.2.2 Broj potrebnih osoba po zadatku

Bezbednosna i operativna regulativa Pružaoca usluga očuvanja definiše da se sledeći poslovi mogu obavljati samo u zaštićenom okruženju, uz istovremeno prisustvo dva zaposlena koji imaju uloge od poverenja:

- Promena sistemskih parametara na nivou baze podataka
- Promena sistemskih parametara na aplikativnom nivou
- Promena infrastrukture

Najmanje jedno od lica koja obavljaju gore navedene procedure mora biti administrator sistema ili inženjer baze podataka, a drugo lice ne može biti nezavisni revizor sistema.

5.2.3 Identifikacija i autentifikacija za svaku ulogu

Korisnici koji su odgovorni za upravljanje IT sistemom Pružaoca usluge čuvanja poseduju jedinstvene identifikacione podatke, pružajući pouzdanu osnovu za bezbednu identifikaciju i autentifikaciju svakog korisnika. Pristup kritičnim IT sistemima, relevantnim za pružanje usluge sertifikacije, je dozvoljen tek nakon uspešne identifikacije i autentifikacije. Identifikacioni i autentifikacioni podaci se momentalno opozivaju u slučaju prestanka prava pristupa korisnika.

Svaki pojedinačni korisnik IT sistema i svaki učesnik u administrativnom procesu je jasno identifikovan, pružajući transparentnost i pojednostavljujući praćenje aktivnosti unutar sistema.

5.2.4 Uloge koje zahtevaju razdvajanje dužnosti

Zaposleni kod Pružaoca usluga čuvanja mogu imati više pouzdanih uloga u isto vreme, ali Pružalac usluga čuvanja obezbeđuje da:

- službenik za bezbednost neće imati ulogu nezavisnog revizora sistema;
- administrator sistema neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema;
- menadžer implementacije sa opštom odgovornošću za IT sistem neće imati ulogu službenika za bezbednost i nezavisnog revizora sistema.

Pored navedenog, Pružalac usluga čuvanja traži potpuno razdvajanje uloga od poverenja.

5.3 Kontrola osoblja

Pružalac usluga čuvanja pažljivo vodi računa o kadrovskoj politici i praksama zapošljavanja članova osoblja, sa fokusom na pojačavanje i podršku pouzdanosti rada. Mere predostrožnosti usmerene na osoblje imaju za cilj smanjenje rizika od ljudskih grešaka, krađe, prevare i zloupotrebe.

Već tokom procesa zapošljavanja, Pružalac usluga čuvanja posvećuje posebnu pažnju bezbednosti osoblja, uključujući zaključivanje ugovora i njihovu validaciju nakon što postanu zaposleni. Kandidati za uloge od poverenja moraju posedovati važeću potvrdu o neosuđivanosti prilikom podnošenja

prijave. Za sve zaposlene u ulogama od poverenja i spoljne strane koje dolaze u kontakt sa uslugama Pružaoca usluga čuvanja, obavezno je potpisivanje ugovora o neotkrivanju podataka.

Paralelno s tim, Pružalac usluga čuvanja garantuje da njegovi zaposleni stiču i kontinuirano unapređuju zajedničko, opšte znanje, zajedno s specijalizovanim stručnim znanjem neophodnim za obavljanje raznovrsnih poslova.

5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje

"Iron Mountain d.o.o." se stara da zaposleni koji upravljaju IKT sistemom, odnosno zaposleni koji koriste IKT sistem imaju adekvatan stepen obrazovanja i sposobnosti, kao i svest o značaju poslova koje obavljaju. Njihove odgovornosti su utvrđene Ugovorom o radu, i Pravilnikom o sistematizaciji sa opisima radnih mesta sa utvrđenim odgovornostima (za rad van radnog odnosa ugovor o delu sa priloženim opisom posla u skladu sa pozicijom (iz sistematizacije).

5.3.2 Procedure provere

"Iron Mountain d.o.o." sprovodi postupke radi provere ispunjenosti uslova svakog pojedinačnog kandidata za zaposlenje, u skladu s odgovarajućim propisima i etičkim smernicama, proporcionalno poslovnim zahtevima, klasifikaciji informacija kojima će imati pristup, i sagledanim potencijalnim rizicima.

Svi zaposleni i angažovani pojedinci po drugom osnovu koji imaju dodeljen pristup poverljivim informacijama, obavezni su potpisati sporazum o poverljivosti i zaštiti podataka i informacija od trećih lica pre nego što im se odobri pristup opremi za obradu informacija.

Da li će u vreme imenovanja nosilac vodeće uloge, zaposlenik Pružaoca usluga čuvanja, izjavom, službenik nosioca uloge od poverenja sa sertifikatom o dobrom ponašanju starom manje od 3 meseca, opravdati čist krivični dosije. Pružalac usluge čuvanja proverava autentičnost relevantnih informacija navedenih u biografiji kandidata tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovne kvalifikacije.

5.3.3 Zahtevi za obuku

Pružalac usluga čuvanja obučava novozaposlene odgovarajućim obukama tokom kojih oni stiču sva potrebna znanja.

Tokom obuke novozaposlenima će biti pruženja znanja i procedure pokrivena sledećim dokumentima:

- "Procesi i procedure definisane u javnim i internim propisima Pružaoca usluge čuvanja"
- "Pravila o zaštiti podataka"
- "Specifičnosti i način rukovanja IT sistemom Pružaoca usluga čuvanja"
- "Neophodna posebna znanja za ispunjavanje njihovog delokruga"
- "Pravne posledice pojedinačnih aktivnosti"
- "Primenljivi IT bezbednosni propisi u meri u kojoj je to neophodno za specifičan obim aktivnosti"

Samo zaposleni koji su prošli obuku dobijaju pristup proizvodnom IT sistemu Pružaoca usluge čuvanja.

5.3.4 Učestalost i uslovi prekvalifikacije

Pružalac usluge čuvanja obezbeđuje da zaposleni stalno poseduju neophodna znanja, pa se po potrebi održavaju dalje ili ponovljene obuke. Dalja obuka se održava ako dođe do promene u procesima ili IT sistemu Pružaoca usluge čuvanja. Obuka je adekvatno dokumentovana, iz čega se jasno može odrediti nastavni plan i obim zaposlenih učesnika.

5.3.5 Učestalost i redosled rotacije poslova

Pružalac usluga čuvanja ne primenjuje obaveznu rotaciju između pojedinačnih rasporeda rada.

5.3.6 Sankcije za nedozvoljene radnje

Pružalac usluga čuvanja precizno reguliše mogućnosti krivičnog gonjenja svojih zaposlenih putem ugovora o radu u slučaju eventualnih propusta, grešaka ili namernog oštećenja. U situaciji da zaposleni, iz nehata ili s namerom, prekrši svoje radne obaveze, Pružalac usluga čuvanja ima pravo da izrekne odgovarajuće sankcije, prilagođene ozbiljnosti prekršaja i njegovim posledicama. Ove

sankcije obuhvataju disciplinske postupke, razrešenje dužnosti, opoziv imenovanja i, ukoliko je potrebno, krivičnu odgovornost.

Prilikom imenovanja, svaki zaposleni od poverenja prima pismene informacije o zakonskim obavezama, pravima, sertifikaciji i standardima upravljanja vezanim za tretman ličnih podataka. Takođe, dobija detaljan opis poslova koji uključuje i bezbednosne zadatke. Potpisivanjem ugovora o poverljivosti, zaposleni se upoznaje s posledicama nepoštovanja bezbednosnih mera, uključujući i eventualne krivične sankcije.

Ove odredbe obuhvataju radno zakonodavstvo, kao i krivične posledice koje se primenjuju u slučaju kršenja zakona, osiguravajući tako poštovanje radnih obaveza i disciplinu unutar organizacije.

5.3.7 Zahtevi nezavisnog izvođača

Pružalac usluga čuvanja pažljivo određuje samo pouzdane uloge za svoje zaposlene. Odabir zaposlenih sa ugovorom o angažovanju ili pod ugovorom za obavljanje specifičnih zadataka vrši se preferencijalno iz liste prethodno kvalifikovanih dobavljača. Pre početka saradnje, Pružalac usluga čuvanja zaključuje pismeni ugovor sa dobavljačima.

Svaka strana u ugovoru, pre nego što preuzme aktivnu ulogu, obavezna je potpisati izjavu o poverljivosti. Ovom izjavom se saglašava da se poslovne i korporativne tajne neće otkrivati neovlašćenim licima niti zloupotrebljavati na bilo koji način. Osim toga, utvrđuju se sankcije koje će biti primenjene u slučaju kršenja ovih pravila. Kada su u pitanju spoljni zaposleni po ugovoru, očekuje se da već poseduju odgovarajuće tehničke veštine, a Pružalac usluga čuvanja ne obezbeđuje posebnu obuku za njih.

5.3.8 Dokumentacija dostavljena osoblju

Pružalac usluge čuvanja kontinuirano obezbeđuje zaposlenima dostupnost aktuelne dokumentacije i propisa neophodnih za obavljanje njihovih uloga. Svi zaposleni se pisanim obaveštenjem obaveštavaju o promenama organizacionih bezbednosnih propisa.

Svaki zaposleni u pouzdanoj ulozi dobija sledeće dokumente u pisanoj formi:

- organizacioni bezbednosni propisi Pružaoca usluge čuvanja,
- potpisati ugovor o poverljivosti,
- lični opis posla,
- edukativni materijali povodom planirane ili posebne obuke za određeni oblik obrazovanja.

5.4 Procedure evidentiranja revizije

5.4.1 Vrste snimljenih događaja

Pružalac usluge čuvanja evidentira svaki događaj vezan za bezbednost koji može da pruži informacije o događajima, promenama koje se dešavaju u IT sistemu ili u njegovom fizičkom okruženju u skladu sa praksom bezbednosti informacija.

Pružalac usluge čuvanja, čuva sledeće podatke:

- vreme događaja
- vrsta događaja
- identifikacija korisnika ili sistema koji/šta je pokrenulo događaj
- dodatne parametre vezan za događaj
- uspeh ili neuspeh događaja

Svi novi zapisi revizije se dodaju zapisima revizije. Ranije sačuvani zapisi revizije ne mogu se menjati ili brisati. Svi bitni zapisnici događaja dostupni su nezavisnim revizorima sistema, koji ispituju usklađenost rada Pružaoca usluge očuvanja.

Pružalac usluge čuvanja evidentira najmanje sledeće događaje:

Administracija korisnika:

- kreiranje korisnika
- brisanje neaktiviranih korisnika
- aktivacija korisnika
- deaktivacija korisnika
- promena lozinke
- kreiranje grupe korisnika
- brisanje grupe korisnika
- dodavanje korisnika u grupa
- brisanje korisnika iz grupe

Ove aktivnosti se čuvaju u bazi podataka i dostupne su administratoru Pretplatnika iz aplikacije.

Rad sa dokumentima:

- kreiranje foldera
- otpremanje dokumenta
- promena meta-podataka dokumenta
- pretvaranje dokumenta u LTA format
- brisanje dokumenta koji nije pripremljen za arhivu
- premeštanje dokumenta iz jednog foldera u drugi
- promena privilegija na folderu ili dokumentu
- preuzimanje dokaza o čuvanju
- preuzimanje elektronskog dokumenata

Ove aktivnosti se čuvaju u bazi podataka i dostupne su administratoru Pretplatnika iz aplikacije.

Prijava korisnika na sistem:

- svaka uspešna i neuspešna prijava, IP adresa i korisnički nalog sa kojim je pokušana prijava za rad na sistemu

broj neuspešnih logovanja sa neke IP adrese, vreme između dva logovanja sa iste adrese se eksponencijalno povećava

Ove aktivnosti se čuvaju u bazi podataka i dostupne su Administratoru sistema.

Aplikativni logovi:

- logovi aplikacije - sadrže datum i vreme, nivo poruke (debug, informativna poruka, upozorenje ili greška), programski modul, detalje poruke

- logovi svih komponenti sistema (baza podataka, DMS, LDAP baza korisnika...)
- logovi se automatski arhiviraju i brišu posle predefinisano perioda

Svi aplikativni logovi su dostupni Administratoru sistema.

Dnevnik promena aplikativnih verzija:

- vreme spuštanja nove verzije aplikativnog rešenja
- kratke informacije o promenama implementiranim u novoj verziji rešenja

Dnevnik promena parametara okruženja:

- promene verzija i parametara komponenta rešenja (parametri baze podataka, DMS-a...)
- promene konfiguracionih parametara rešenja

Dnevnik sinhronizacije vremena:

- sinhronizaciju internog sata sa UTC vremenom
- izveštaj promene kalibracije
- izveštaj gubitka sinhronizacije

Dnevnik promena na serverskom okruženju:

- promena hardvera ili pojedinih hardverskih komponenti
- ažuriranje verzije operativnog sistema
- primena zakrpa (patch)
- restart servera sa razlogom restarta

Dnevnik problema u radu sistema:

- problemi u nedostupnosti softverskog rešenja
- problemi u funkcionisanju softverskog rešenja
- problem u radu operativnog sistema
- hardverski problemi
- problemi u napajanju električnom energijom
- problemi u mrežnoj infrastrukturi
- detekcija mrežnih ili drugih napada na sistem

Dnevnik fizičkog pristupa:

- pristup ovlašćenih osoba fizičkoj infrastrukturi
- pokušaj pristupa neovlašćenih osoba fizičkoj infrastrukturi

5.4.2 Učestalost obrade dnevnika zapisa

Nezavisni sistemski revizori Pružaoca usluge čuvanja redovno ocenjuju generisane datoteke evidencije svakog radnog dana. Ovaj proces obezbeđuje autentičnost i integritet pregledanih dnevnika, s posebnim fokusom na proveru poruka o greškama u evidenciji. U slučaju detektovanih odstupanja, revizori dokumentuju razlike i preduzimaju mere kako bi otklonili uzroke neregularnosti.

Svi rezultati inspekcije, istraživanja i preduzete mere za otklanjanje identifikovanih nedostataka se pažljivo dokumentuju, obezbeđujući transparentnost i praćenje akcija koje su preduzete radi poboljšanja sistema.

5.4.3 Period zadržavanja za evidenciju revizije

Dnevnici se redovno arhiviraju po usvojinim polisama za bekap i arhiviranje, a Pružalac usluge čuvanja garantuje njihovo sigurno čuvanje tokom vremenskog perioda definisanog u odeljku 5.5.2, ali najmanje 10 (deset) godina od trenutka njihovog nastanka. Tokom tog perioda, Pružalac usluge čuvanja održava čitljivost arhiviranih podataka i održava potrebne softverske i hardverske alate za tu svrhu, i obezbeđuje zaštitu od neovlašćenog pristupa.

5.4.4 Zaštita dnevnika zapisa

Pružalac usluge čuvanja štiti kreirane dnevnike za potrebno vreme čuvanja. Tokom čitavog vremena čuvanja, obezbeđuju se sledeća svojstva podataka dnevnika:

- zaštita od neovlašćenog otkrivanja: samo ovlašćena lica – prvenstveno nezavisni revizori sistema – pristupaju evidencijama;
- dostupnost: ovlašćenim licima je odobren pristup evidenciji;
- integritet: sprečena je svaka promena podataka, brisanje u fajlovima evidencije i promena redosleda unosa itd.

Datoteke evidencije su zaštićene od slučajnog i zlonamernog oštećenja rezervnim kopijama. U slučaju unosa u dnevnik koji sadrže lične podatke, Pružalac usluge čuvanja vodi računa o poverljivom čuvanju podataka. Samo oni pojedinci imaju pravo pristupa unosima u dnevnik, kojima je to apsolutno

potrebno za njihov rad. Pružalac usluge čuvanja verifikuje pristupe na bezbedan način. Pružalac usluge čuvanja čuva datoteke evidencije u bezbednom okruženju. Čuva kopije datoteka na drugom mestu operacije.

5.4.5 Procedure rezervne kopije dnevnika zapisa

Dnevni log fajlovi nastaju kroz neprekidne unose dnevnika tokom operacija u sistemu. Nakon evaluacije, ove datoteke dnevnih evidencija se arhiviraju u dve kopije i čuvaju fizički odvojeno jedna od druge, na različitim lokacijama, tokom određenog vremenskog perioda.

5.4.6 Obaveštenje subjektu koji izaziva događaj

Osobe, organizacije i aplikacije odgovorne za izazivanje događaja greške nisu uvek obavestene, ali kada je potrebno, Pružalac usluge čuvanja ih uključuje u istraživanje događaja. Klijenti koji su pogođeni događajem su dužni saradivati s Pružaocem usluge čuvanja kako bi zajedno istražili uzrok događaja.

5.4.7 Procene ugroženosti

Pružalac usluge čuvanja aktivno prati svakodnevnu obradu sistemskih zapisa i prati javno dostupne informacije o potencijalnim ranjivostima i sigurnosnim ažuriranjima softverskih paketa. Takođe, vrši analizu ovih informacija, klasifikuje ranjivosti i obaveštava menadžment o rezultatima, predlažući potrebne korake za unapređenje bezbednosti sistema.

U slučaju značajnih propusta koji su otkriveni ili u prisustvu spoljne pretnje, Pružalac usluge čuvanja obaveštava odgovarajuće instance u roku od 48 sati od njihovog otkrivanja, ali najmanje jednom godišnje vrši sveobuhvatnu analizu ranjivosti. Ova analiza uključuje mapiranje potencijalnih unutrašnjih i eksternih pretnji koje bi mogle rezultirati neovlašćenim pristupom.

Na osnovu rezultata analize Pružalac usluge čuvanja:

- kreira i sprovodi plan za ublažavanje ugroženosti ili
- dokumentuje činjeničnu osnovu za odluku da je preostali rizik prihvaćen i da ugroženost ne zahteva sanaciju.

Najpre se nove verzije softvera i sigurnosnih dopuna softverskih rešenja instaliraju na test sistem Pružaoca usluge čuvanja, a tek nakon uspešno završenog testa se instaliraju na živi sistem koji se koristi za pružanje usluga.

Nove sigurnosne dopune softverskih rešenja se ne instaliraju na sistem uživo ako unose dodatne ranjivosti ili nestabilnosti koje prevazilaze prednosti njihove primene. Razlozi za neprimenjivanje bezbednosnih dopuna su dokumentovani.

5.5 Arhivski zapisi

5.5.1 Vrste arhiviranih zapisa

Pružalac usluge čuvanja arhivira sledeće vrste informacija:

- svaki dokument u vezi sa akreditacijom Pružaoca usluge čuvanja;
- sve izdate verzije Politika čuvanja;
- sve izdate verzije Praktičnih pravila čuvanja;
- sve izdate verzije Opštih uslova;
- ugovori u vezi sa radom Pružaoca usluge čuvanja;
- svaki elektronski i papirni unos u dnevnik.

5.5.2 Period čuvanja arhive

Pružalac usluge čuvanja čuva arhivirane podatke za dole navedene vremenske periode:

- Politiku kvalifikovanog čuvanja u trajanju od najmanje 10 godina od datuma ukidanja;
- Praktična pravila čuvanja najmanje 10 godina od datuma ukidanja;

- Opšti uslovi poslovanja najmanje 10 godina od dana prestanka;
- Svi ostali dokumenti da se arhiviraju najmanje 10 godina od dana nastanka

5.5.3 Zaštita arhive

Pružalac usluge čuvanja čuva arhivirane podatke u dve kopije na različitim infrastrukturnim instancama.

Prilikom čuvanja arhiviranih podataka obezbeđuje se sledeće:

- kontinuirana dostupnost podataka
- integritet podataka
- zaštita od neovlašćenog pristupa podacima
- čuvanje autentičnosti podataka

5.5.4 Procedure arhiviranja rezervnih kopija

Pružalac usluge čuvanja čuva elektronske dokumente, metapodatke i dokaze o čuvanju. Takođe, radi se i arhiviranje rezervnih kopija neophodnih softverskih komponenti i podataka.

Procedura arhiviranja rezervnih kopija opisana je u okviru internih procedura.

5.5.5 Zahtevi za postavljanje vremenskog žiga na zapise

Svaki zapis ima vremensku oznaku, na kojoj je vreme koje je obezbedio sistem naznačeno sa tačnošću od najmanje jedne sekunde.

Na ovaj način Pružalac usluge čuvanja garantuje da je odstupanje vremena naznačenog u vremenskim oznakama od UTC vremenske baze najviše 1 sekundu.

5.5.6 Procedure za dobijanje i verifikaciju arhivskih informacija

Pružalac usluge čuvanja kreira datoteke evidencije ručno ili automatski. U slučaju automatskog sistema evidentiranja, datoteke evidencije se generišu svakodnevno. Arhivirane datoteke su zaštićene od neovlašćenog pristupa.

Kontrolisani pristup arhiviranim podacima dostupan je samo kvalifikovanim licima: Klijenti imaju pravo da vide uskladištene podatke koji im odgovaraju; u pravnim sporovima radi pružanja dokaza dostavljaju se potrebni podaci

5.6 Kompromis i oporavak od katastrofe

U slučaju havarije, Pružalac usluge čuvanja preduzima sve neophodne mere kako bi minimizirao štetu nastalu usled nedostatka usluge, i vraća usluge u najkraćem mogućem roku.

Na osnovu procene incidenta koji se dogodio, preduzima potrebne izmene, korektivne mere kako bi se sprečio nastanak incidenta u budućnosti.

Kada se problem reši, događaj se prijavljuje nadležnom Ministarstvu, kao nadzornom organu.

5.6.1 Procedure za rukovanje incidentima

Pružalac usluge čuvanja ima plan kontinuiteta poslovanja.

Pružalac usluge čuvanja uspostavlja i održava potpuno funkcionalan rezervni sistem koji je sposoban da preuzme funkcionalnosti u slučaju otkazivanja primarnog sistema.

Pružalac usluge čuvanja svake godine testira prelazak na rezervni sistem i pregleda svoje planove za kontinuitet poslovanja.

Pružalac usluge čuvanja je povećao bezbednosne alate i sisteme kako bi sveo na minimum greške softvera i hardvera i oštećenja podataka. Povratnost usluga je zagarantovana osnovnim ugovorima i sopstvenim alatima za rezervne kopije Pružaoca usluge čuvanja.

Pružalac usluge čuvanja je konstruisao svoj IT sistem koji pruža usluge poverenja na način da u slučaju ispadanja bilo kog uređaja može da nastavi pružanje usluga od poverenja.

5.6.2 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Zadaci koji se izvršavaju u slučaju kvara usluge usled elementarne nepogode ili drugih nepogoda detaljno su definisani u planu za kontinuitet poslovanja Pružaoca usluge čuvanja. U situaciji havarije, plan se aktivira u skladu sa procedurama opisanim u njemu.

5.7 Prestanak rada pružaoca kvalifikovane usluge od poverenja

"Iron Mountain d.o.o." će, u slučaju planiranog prestanka pružanja usluga od poverenja:

- obavestiti sve korisnike usluga, treće strane i nadležni organ državne uprave najmanje 60 dana pre planiranog prestanka pružanja usluga od poverenja,
- uložiti sav napor da kod drugog kvalifikovanog pružaoca usluga od poverenja osigura nastavak pružanja usluga i tom pružaocu usluga dostaviti svu potrebnu dokumentaciju
- u slučaju prestanka pružanja usluga "Iron Mountain d.o.o." će arhivirati, zaštititi i čuvati zapise kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu sa važećom zakonskom regulativom, ili će sa drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.



Nakon prestanka usluge, Pružalac usluge čuvanja predaje Pretplatniku arhivirane dokumente i dokaze čuvanja i briše ih iz svoje arhive na nepovratan način.

6. Tehničke bezbednosne kontrole

6.1 Opšti zahtevi

Opšti zahtevi “Iron Mountain d.o.o.” obezbeđuje odgovarajuću zaštitu imovine, uključujući i informacionu imovinu, koja se upotrebljava za pružanje usluga od poverenja i u tu svrhu vodi celokupni popis imovine sa pripadajućom klasifikacijom koja je u skladu sa procenom rizika. Mere fizičke zaštite, postupci koje “Iron Mountain d.o.o.” primenjuje u zaštiti sistema za pružanje usluga od poverenja, kao i postupci upravljanja i provere sistema su interne prirode i njihovi detalji se ne objavljuju javno.

6.2 Kontrola pristupa

“Iron Mountain d.o.o.” implementira specifične bezbednosne kontrole pristupa računarima koji se koriste u okviru informacionog sistema Pružaoca kvalifikovane usluge od poverenja. Neautorizovan pristup računarima u okviru informacionog sistema nije dozvoljen.

Računarska i komunikaciona oprema koja se koristi u okviru pružaoca kvalifikovane usluge od poverenja fizički je obezbeđen. Pristup računarskoj mreže se štiti pomoću specijalnih firewall uređaja u skladu sa pružaocem usluge Data centra.

Opšti uslovi Data centra od 1.6.2021. godine, primenjeni na ugovorni odnos između “Iron Mountain d.o.o.” i Data Cloud Technologies, jasno propisuju obaveze u vezi sa čuvanjem poverljivosti podataka, zaštitom ličnih podataka, uslovima prihvatljivog korišćenja, kao i pružanjem usluga u skladu sa nivoom usklađenosti (SLA), čime se uspostavlja temeljna osnova za sistematsko i efikasno sprovođenje fizičke sigurnosti u Data centru.

6.2.1 Bezbednost operacija

U cilju održavanja ispravnog funkcionisanja usluge kvalifikovanog čuvanja elektronskih dokumenata, "Iron Mountain d.o.o." vrši testiranja procesa čuvanja, funkcionalne logike, korisničkog interfejsa i bezbednosnih procedura pre puštanja u rad, kao i prilikom svake izmene funkcionalnosti u softveru ili hardveru koji podržava proces kvalifikovanog čuvanja elektronskih dokumenata.

Razvojno, testno i produkciono okruženje "Iron Mountain d.o.o." su striktno razdvojeni, posebno se održavaju i ne preklapaju se ni u jednom segmentu.

Sve ključne informacije vezane za operacije u okviru pružaoca usluge se backup-uju u skladu sa odredbama Politike pružanja kvalifikovanih usluga od poverenja i odgovarajućih praktičnih pravila rada.

"Iron Mountain d.o.o." vrši prikupljanje evidencionih podataka i audit logova kako je naznačeno u odeljku 5.4 ovog dokumenta.

6.3 Kontrole kompjuterske bezbednosti

6.3.1 Specifični tehnički zahtevi za bezbednost računara

Bezbednost računarske mreže "Iron Mountain d.o.o." zasnovana je na konceptu segmentacije mreže na mrežne zone različitih nivoa. Mrežne zone razgraničavaju se zaštitnim mehanizmima koji propuštaju samo neophodan mrežni saobraćaj.

Na sve sisteme locirane unutar jedne mrežne zone primenjuju se iste bezbednosne mere. Mrežni segment u kome se nalaze radne stanice za administraciju odvojen je od ostalih mrežnih segmenta i računara koji se nalaze u tim mrežnim segmentima.

Oprema za zaštitu računarske mreže beleži tok saobraćaja i pokušaje pristupa servisima i javnim internet stranicama.

Samo ovlašćena lica sa poverljivim ulogama imaju administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže nije dozvoljeno.

Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računarska mreža zaštićena je od neovlašćenog pristupa, uključujući i pristup korisnika i trećih lica.

Mrežne komponente čuvaju se u fizički i logički bezbednom okruženju i usaglašenost njihove konfiguracije periodično se proverava.

6.3.2 Ocena računarske bezbednosti

U cilju održavanja visokog nivoa usluga, "Iron Mountain d.o.o." poseduje zvanične ISO sertifikate i to:

- sistem kontrole kvaliteta u skladu sa standardom ISO 9001
- sistem upravljanja bezbednošću informacija ISO/IEC 27001

Procena rizika se ažurira najmanje jednom godišnje.

Na osnovu rezultata procene rizika Pružalac usluge čuvanja sprovodi sledeće akcije:

- postavlja nove mere za uklanjanje ranjivosti ili/i
- prihvata identifikovane preostale rizike navodeći razlog za odluku.

7. Revizija usklađenosti i druge procene

Pružanje usluge "Iron Mountain d.o.o." je pod nadzorom Ministarstva informisanja i telekomunikacija, u skladu sa propisima Evropske unije. Ministarstvo informisanja i telekomunikacija sprovodi godišnju inspekciju na lokaciji Pružaoca usluge. Pre inspekcije, "Iron Mountain d.o.o." angažuje eksternog revizora za sprovođenje skrininga poslovanja i šalje detaljan izveštaj Ministarstvu informisanja i telekomunikacija u roku od 3 dana od dana prijema.

Skrining se sprovodi radi provere da li rad Pružaoca usluga kvalifikovanog elektronskog čuvanja dokumenata udovoljava zahtevima eIDAS Uredbe, kao i pripadajućih srpskih zakona i zahteva primenjene Politike kvalifikovanog elektronskog čuvanja dokumenata i odgovarajućih Praktičnih pravila kvalifikovanog elektronskog čuvanja dokumenata. Cilj je osigurati da Pružalac usluge čuvanja ispunjava sve relevantne standarde i propise kako bi se garantovala sigurnost i integritet čuvanih podataka.

Rezultat skrininga predstavlja poverljiv dokument dostupan isključivo ovlašćenim pojedincima.

Sertifikat o usaglašenosti, izdat u skladu sa izveštajem o ocenjivanju usaglašenosti, javno se objavljuje na internet stranici <https://digidocs.rs/dokumenti/>.

Svaki element sistema korišćen za pružanje usluga klasifikovan je prema bezbednosnim klasama putem procene rizika sprovedene od strane "Iron Mountain d.o.o.". Detaljna evidencija o ovim sistemskim elementima i povezanim bezbednosnim ocenama čuva se unutar sistema upravljanja rizikom od strane "Iron Mountain d.o.o."

Osim spoljne revizije, "Iron Mountain d.o.o." održava vlastiti sistem interne revizije koji redovno ocenjuje usaglašenost sa prethodnim revizijama. U slučaju identifikacije odstupanja, preduzimaju se odgovarajući koraci kako bi se osigurala ispravka.

Pružalac usluge čuvanja integriše sistem upravljanja kvalitetom u skladu sa ISO 9001. Takođe, poseduje sistem upravljanja bezbednošću informacija u skladu sa ISO 27001 (prethodno poznat kao BS 7799). Ovi sistemi se kontinuirano revidiraju i pregledavaju od strane eksterne revizorske organizacije.

7.1 Procena učestalosti

Svake godine "Iron Mountain d.o.o." vrši procenu usaglašenosti na svom IT sistemu koji obavlja pružanje usluga.

7.2 Identifikacija/Kvalifikacije procenjivača

"Iron Mountain d.o.o." sprovodi interne revizije putem svojih zaposlenih koji obavljaju ulogu nezavisnih revizora sistema.

Ocenu usklađenosti sa zakonskom regulativom i ETSI standardima sprovodi nadležno ministarstvo.

7.3 Odnos procenitelja prema procenjenom subjektu

Eksternu reviziju sprovodi osoba koja:

- poseduje nezavisnost u odnosu na vlasnike, menadžment i operativne aktivnosti ispitanoг pružaoca usluge čuvanja.
- treba da bude nezavisna u odnosu na ispitivanu organizaciju, tj. ni ona ni njeni najbliži rođaci nemaju nikakav radni ili poslovni odnos sa "Iron Mountain d.o.o."
- njena naknada ne zavisi od rezultata aktivnosti sprovedenih tokom revizije.

7.4 Tematski opseg procene

Pregled obuhvata sledeće aspekte:

- Usklađenost sa važećim zakonima.
- Usklađenost sa tehničkim standardima.
- Usklađenost sa Politikom sertifikacije i Praktičnim pravilima kvalifikovanog čuvanja.
- Adekvatnost sprovedenih procesa.
- Integritet i tačnost dokumentacije.
- Procena fizičke bezbednosti.
- Ocena adekvatnosti osoblja.
- Evaluacija IT bezbednosti.
- Usaglašenost sa pravilima zaštite podataka.



7.5 Postupci nakon otkrivanja nedostataka

Nezavisni revizor predstavlja rezultate pregleda u opsežan izveštaj o skriningu koji obuhvata testirane komponente sistema, procese i pruža dokaze korišćene tokom skrininga, uz revizorske izjave. Neusaglašenosti identifikovane tokom ispitivanja, zajedno s rokovima za njihovo otklanjanje, dokumentuju se u posebnom delu izveštaja.

8. Reference

- Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju (Službeni glasnik RS, br. 94 od 19. oktobra 2017, 52 od 24. maja 2021.)
- Zakon o arhivskoj građi i arhivskoj delatnosti Republike Srbije (Službeni glasnik RS, br. 6 od 24. januara 2020.)
- Zakon o informacionoj bezbednosti (Službeni glasnik RS, br. 6 od 28. januara 2016.)
- Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, br. 87 od 13. novembra 2018.)
- Uredba o jedinstvenim tehničko-tehnološkim zahtevima i procedurama za čuvanje i zaštitu arhivske građe i dokumentarnog materijala u elektronskom obliku (Službeni glasnik RS, br. 107 od 12. novembra 2021., br. 94 od 25. avgusta 2022.)
- Uredba o uslovima za pripremu dokumenta za pouzdano elektronsko čuvanje i formatima dokumenta koji su pogodni za dugotrajno čuvanje (Službeni glasnik RS, br)
- Pravilnik o uslovima za postupke i tehnološka rešenja koji se koriste tokom pouzdanog elektronskog čuvanja dokumenta (Službeni glasnik RS, br)
- Pravilnik o validaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (Službeni glasnik RS, br)
- Pravilnikom o bližim uslovima za kvalifikovane elektronske vremenske žigove (Službeni glasnik RS, broj 59/2019)
- Uredba o uslovima za pružanje kvalifikovanih usluga od poverenja ((Službeni glasnik RS, broj 37 od 11. maja 2018)
- ETSI TS 119 512 V1.1.1 (2020-01); Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services (Elektronski potpisi i infrastrukture (ESI); Protokoli za pružaoce usluga poverenja koji pružaju usluge dugoročnog čuvanja podataka)
- ETSI TS 119 441 "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services "
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Uredbe (EU) 910/2014 EVROPSKOG PARLAMENTA I SAVETA od 23. Jula 2014. o elektronskoj identifikaciji i uslugama poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC)

- ETSI TS 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers “
- ETSI SR 019 050 V1.1.1 (2015-06); Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures (Elektronski potpisi i infrastrukture (ESI); Racionalizovan okvir standarda za elektronske usluge registrovane dostave koje primenjuju elektronski potpis)
- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji izdaju vremenske žigove)
- ETSI TS 119 101 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation (Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za aplikacije za kreiranje potpisa i validaciju potpisa)
- ETSI EN 319 522- 1 V1.1.1 (2018-09); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation (Elektronski potpisi i infrastrukture (ESI); Elektronske usluge registrovane isporuke; Deo 1: Okvir i arhitektura)
- ETSI EN 319 522-2 V1.1.1 (2018-09); Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents (; Elektronski potpisi i infrastrukture (ESI); Elektronske usluge registrovane isporuke; Deo 2: Semantički sadržaji)
- ETSI EN 319 521 V1.1.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers (Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce elektronskih registrovanih usluga isporuke)
- ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (Elektronski potpisi i infrastrukture (ESI); Zahtevi politike i bezbednosti za pružaoce usluga od poverenja koji obezbeđuju dugoročno očuvanje digitalnih potpisa ili opštih podataka korišćenjem tehnika digitalnog potpisa)
- ETSI TS 119 312 V1.2.1 (2017-05); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- ISO/IEC 27001 - standard for information security management systems (ISMS)
- ETSI TS 119 312 V1.4.1 (2021-08); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites (Elektronski potpisi i infrastrukture (ESI); Kriptografski paketi)

- ETSI TS 119 102-1 V1.2.1 (2018-08); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI TS 119 102-2 V1.3.1 (2021-09); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
- ETSI EN 319 102-1 V1.1.1 (2016-05); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 142-1 V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures (Elektronski potpisi i infrastrukture (ESI); PAdES digitalni potpisi; Deo 1: Građevinski blokovi i PAdES osnovni potpisi)
- ETSI EN 319 142-2 V1.1.1 (2016-04); Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles (Elektronski potpisi i infrastrukture (ESI); PAdES digitalni potpisi; Deo 2: Dodatni profili PAdES potpisa)
- ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
- ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (Elektronski potpisi i infrastrukture (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja)
- Registar pružalaca kvalifikovanih usluga od poverenja – Poverenička lista (<https://mit.gov.rs/tekst/sr/583/registar-pruzalaca-kvalifikovanih-usluga-od-poverenja-.php>)
- ISO 19005-1:2005 – Upravljanje dokumentima – Format elektronske datoteke dokumenta za dugoročno čuvanje – Deo 1: Korišćenje PDF-a 1.4 (PDF/A-1).
- Politika pružanja kvalifikovanih usluga od poverenja Sertifikacionog tela Privredne komore Srbije (<http://v3.pksc.rs/docs/CP%20PKSCA.pdf>)
- Praktična pravila rada za pružanje kvalifikovane usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u (<http://v3.pksc.rs/docs/CPS%20PKSCA%20CLOUD.pdf>)
- Praktična pravila rada za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (<http://v3.pksc.rs/docs/CPS%20PKSCA%20UPRAVLJANJE%20SREDSTVOM%20ZA%20KREIRANJE%20POTPISA.pdf>)

- Politika i praktična pravila rada za pružanje kvalifikovane usluge validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (<http://v3.pksc.rs/docs/CPS%20PKSCA%20VALIDACIJA.pdf>)
- Praktična pravila rada za pružanje kvalifikovane usluge izdavanja kvalifikovanih elektronskih vremenskih žigova (<http://v3.pksc.rs/docs/CPS%20PKSCA%20TSA.pdf>)

9. Istorija rada dokumenta

Naziv	Vrednost
OID broj dokumenta	1.3.6.1.4.1.16100.66100.1.1
Važi od:	15.11.2023.

Verzija:	1.0
Datum verzije:	15.11.2023.
Autori:	Andrija Martić - Kontrola kvaliteta Darko Simonović - Sistem administrator Nenad Maksimović – Direktor prodaje razvoja i strategije
Nivo poverljivosti:	Javno
Odgovorna osoba:	Benil Misini, direktor

Izdanje	Broj dokumenta	Verzija	Datum	Opis promene	Izmene pripremio	Izmene odobrio
1.	1.3.6.1.4.1.161 00. 66100.1.1	1.0	15.11.2023.	Inicijalna verzija	Darko Simonović	Benil Misini