Na osnovu člana 7 i 8. stav 1. Zakona o informacionoj bezbednosti („Službeni glasnik RS", broj 6/16, 94/17 i 77/19), čl. 2. i 3 kao i u skladu sa zahtevima ISO-IEC 27001:2013 načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema („Službeni glasnik RS", broj 94/16), odnosno kojima su definisani nadležnosti, poslovi i ovlašćenja, rukovodstvo "Iron Mountain d.o.o." donosi

Akt o bezbednosti informaciono-komunikacionog sistema Operatora IKT sistema

"Iron Mountan d.o.o."

OSNOVNE ODREDBE

Predmet Akta
Član 1.

Aktom o bezbednosti informaciono-komunikacionog sistema Iron Mountain d.o.o. (u daljem tekstu: Akt o bezbednosti), u skladu sa Zakonom o informacionoj bezbednosti („Službeni glasnik RS", broj 6/16, 94/17 i 77/19, u daljem tekstu: Zakon), bliže se uređuju mere zaštite, principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima informaciono-komunikacionog sistema "Iron Mountain d.o.o." (u daljem tekstu: IKT sistem).

Ciljevi Akta o bezbednosti
Član 2.

Ciljevi donošenja Akta o bezbednosti su:

1. određivanje načina i procedura za postizanje i održavanje adekvatnog nivoa bezbednosti sistema;

2. sprečavanje i ublažavanje posledica incidenata kojim se ugrožava ili narušava informaciona bezbednost;
3. podizanje svesti kod zaposlenih o značaju informacione bezbednosti, rizicima i merama zaštite prilikom korišćenja IKT sistema;
4. propisivanje ovlašćenja i odgovornosti zaposlenih u vezi sa bezbednošću i resursima IKT sistema;
5. sveukupno unapređenje informacione bezbednosti i provera usklađenosti primene mera zaštite.

Obaveza primene odredbi Akta o bezbednosti

Član 3.

Mere zaštite IKT sistema koje su bliže uređene Aktom o bezbednosti služe prevenciji od nastanka incidenata i minimizaciji štete od incidenata i njihova primena je obavezna za sve zaposlene i radno nagažovane. Zaposleni i radno angažovani u "Iron Mountain d.o.o." moraju biti upoznati sa sadržinom Akta o bezbednosti i dužni su da postupaju u skladu sa odredbama ovog akta, kao i drugih internih procedura koje regulišu informacionu bezbednost. "Interni revizor , "Menadžer Implementacije "i "Izvršni Direktor" odgovorni su za praćenje primene mera bezbednosti, kao i za proveru da su podaci zaštićeni na način koji je utvrđen ovim aktom i internim procedurama.

Odgovornost zaposlenih

Član 4.

Zaposleni i radno angažovani u "Iron Mountain d.o.o." su dužni da pristupaju informacijama i resursima IKT sistema samo radi obavljanja redovnih poslovnih aktivnosti, kao i da blagovremeno informišu ovlašćeno lice o svim sigurnosnim incidentima i problemima. Nepoštovanje odredbi Akta o bezbednosti, kao i svako ugrožavanje ili narušavanje informacione bezbednosti, povlači disciplinsku odgovornost zaposlenog.

Predmet zaštite
Član 5.

Mere zaštite IKT sistema odnose se na:

- elektronske komunikacione mreže,
- elektronske uređaje na kojima se čuva i vrši obrada podataka korišćenjem računarskog programa, operativne i aplikativne računarske programe,
- programski kôd, podatke koji se čuvaju, obrađuju, pretražuju ili prenose pomoću elektronskih uređaja,
- organizacionu strukturu putem koje se upravlja IKT sistemom, korisničke naloge, tajne informacije za proveru verodostojnosti, tehničku i korisničku dokumentaciju, unutrašnje opšte akte i procedure.

Sve gore navedeno je nabrojano u "Listi resursa".

Mere zaštite

Svaki član sadrži opis mera zaštite uključujući predloge procedura, ovlašćenja i odgovornosti učesnika u sprovođenju. Svrha ovog Akta je uspostavljanje mera zaštite informacija koje su u skladu sa regulatornim, klijentskim i ugovornim zahtevima i obezbeđuju da štite "Iron Mountain d.o.o." informacije protiv gubitka, neovlašćenog pristupa ili otkrivanja. Merama zaštite IKT sistema se obezbeđuje neovlašćeno otkrivanje, uklanjanje ili uništenje informacija koji se čuvaju na nosačima podataka, kao i prevencija od incidenata koja ugrožavaju obavljanje delatnosti. „Iron Mountain d.o.o" sa ciljem očuvanja bezbednosti informacija koristi tehnicke mere zastite, fizicke mere zaštite, organizacione, kao i kadrovske mere zaštite.

Shodno navedenom, pomenute mere su detaljno opisane u nastavku Modela Akta o Bezbednosti.

Uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema

Član 6.

„Iron Mountain d.o.o.“ u okviru organizacione strukture utvrđuje poslove i odgovornosti zaposlenih u cilju upravljanja informacionom bezbednošću.

Interni akti koji uređuju obaveze i odgovornosti zaposlenih u vezi sa upravljanjem informacionom bezbednošću:

- Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mesta;
- Ugovori o radu;
- Data protection formular;
- Ugovori o čuvanju poverljivosti sa pravnim licima;
- Data privacy formular.

Generalni direktor je dužan da donese pojedinačni akt, u skladu sa aktom o sistematizaciji, kojim određuje odgovorna lica za obezbeđivanje i praćenje bezbednosti informacionog sistema “DigiDocs”. Svi zaposleni moraju biti upoznati sa procedurom zaštite bezbednosti IKT sistema. "Iron Mountain d.o.o." procedurom ” P-014-Kontrola pristupa resursima” utvrđuje način dodele ovlašćenja za pristup IKT sistemu, stepen obuke i kvalifikaciju zaposlenih, način odobravanja pristupa zaposlenima od strane rukovodioca, odnosno neposredno nadređenog lica. Ovom procedurom utvrđuje se i odgovornost svakog zaposlenog i odgovornog lica i propisuje disciplinska odgovornost zaposlenog, u slučaju nepoštovanja odredbi koje uređuju informacionu bezbednost.

Postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja

Član 7.

"Iron Mountain d.o.o." dozvoljava rad na daljinu i upotrebu mobilnih uređaja od strane zaposlenih, ukoliko je osigurana bezbednost rada u slučaju obavljanja poslova van prostorija poslodavca, uzimajući u obzir i rizike do kojih može doći usled neadekvatnog korišćenja mobilnih uređaja.

Rad na daljinu

Radni odnos za obavljanje poslova van prostorija poslodavca obuhvata:

- Rad na daljinu;
- Rad od kuće;
- Virtuelno radno okruženje.

Rad na daljinu u smislu ovog Akta odnosi se na situaciju kada je zaposleni i drugi radno angažovani obavezan da izvrši određene poslove na mreži poslodavca, a nalazi se van prostorija poslodavca.

Predmetno angažovanje i omogućavanje obavljanja zadatih i neophodnih poslova se uređuje putem Procedure za P-014- Kontrola pristupa resursima pristup informacionom sistemu .

Procedura P-014- Kontrola pristupa resursima definiše pravila i uslove za povezivanje na mrežu "Iron Mountain d.o.o." sa udaljene lokacije. Pravilnom primenom utvrđenog postupka i načina pristupa, "Iron Mountain d.o.o." svodi na minimum potencijalnu izloženost šteti koja može nastati usled neautorizovanog ili nekontrolisanog pristupa mreži.

Ova procedura se primenjuje na sve zaposlene u "Iron Mountain d.o.o." i saradnike koji koriste računare ili mobilne uređaje za povezivanje na mrežu "Iron Mountain d.o.o.", i uređuje pristup sa udaljenih lokacija u svrhu obavljanja posla u ime i za račun "Iron Mountain d.o.o.", uključujući korišćenje elektronske pošte i mrežnih resursa, kao i način pristupa mreži "Iron Mountain d.o.o." sa udaljenih lokacija.

Autorizovanim korisnicima nije dozvoljeno da koriste mrežu "Iron Mountain d.o.o." za aktivnosti koje nisu u domenu poslovnih aktivnosti, radnih i drugih zadataka u vezi sa poslom i predmetom rada pojedinačno zaposlenog.

Zahtevi koji moraju biti ispunjeni i definisani u proceduri:

1. Pristup sa udaljenih lokacija mora biti zaštićen korišćenjem kriptografskih algoritama.
2. Autorizovani korisnici moraju čuvati kredencijale svojih naloga i ne smeju omogućiti pristup bilo kom trećem licu.
3. Prilikom korišćenja službenog računara za pristup sa udaljene lokacije mreži "Iron Mountain d.o.o.", autorizovani korisnik ne sme istovremeno biti povezan i na neku drugu mrežu koja može ugroziti bezbednost komunikacije.

4. Pristup sa udaljene lokacije mora biti odobren od strane odgovornog lica za nadzor sprovođenja ove procedure.
5. Svi uređaji koji su povezani na internu mrežu preko udaljenih lokacija moraju imati instaliranu zaštitu u vidu antivirusnog softvera. Treća lica su u obavezi da primenjuju zahteve iz zaključenih ugovora sa "Iron Mountain d.o.o.".
6. Svi poslovni podaci koji se kreiraju prilikom rada na daljinu skladište se u informacionom sistemu. Radi bezbednosti, poslovni podaci se ne skladište na mobilnim uređajima.

Korišćenje mobilnih uređaja

Mobilni uređaji podrazumevaju sve prenosne elektronske uređaje namenjene za komunikaciju na daljinu. U mobilne uređaje spadaju prenosivi računari, tableti, mobilni telefoni, PDA i svi drugi mobilni uređaji koji sadrži podatke i imaju mogućnost povezivanja na mrežu. Prilikom korišćenja mobilnih uređaja potrebno je osigurati poslovne informacije od mogućeg kompromitovanja.

Procedurom "P-017 Pravilna upotreba informatickih resursa" definiše se način fizičke zaštitite od krađe i aktivnosti koje je neophodno preduzeti u slučaju krađe ili gubitka mobilnih uređaja, odnosno bezbednosnog incidenta, kako ne bi bila narušena bezbednost.

Iron Mountain d.o.o. sprovodi obuku zaposlenih koji koriste mobilne uređaje, u cilju podizanja svesti o dodatnim rizicima do kojih dolazi usled ovakvog načina rada.

Procedurom o korišćenju mobilnih uređaja potrebno je ustanoviti sledeća pravila:

1. Svi uređaji moraju biti zaštićeni jakom šifrom.

Naš princip snažne šifre jasno je utvrđen u standardima za identitet i upravljanje pristupom u okviru globalne Iron Mountain procedure. - Identity and Access Management Standard.

2. Krađa ili gubitak mobilnog uređaja se mora bez odlaganja prijaviti nadležnoj organizacionoj jedinici za informacione tehnologije i odgovornom licu, koji zatim sprovode aktivnosti u smislu očuvanja bezbednosti. Ukoliko se uređaj pronađe, potrebno je predati isti odgovornim licima.
3. Korisnicima nije dozvoljeno da vrše izmene na hardveru ili instaliranom softveru koji je vlasništvo "Iron Mountain d.o.o." bez prethodne pisane dozvole sektora za informacione tehnologije i odgovornog lica u sektoru.

4. U cilju zaštite podataka organizaciona jedinica za informacione tehnologije će evidentirati korišćenje mobilnih uređaja u odgovarajućim logovima, koje će u slučaju potrebe koristiti za istraživanja i utvrđivanja eventualnih zloupotreba.

Procedura se primenjuje na sve stalno zaposlene, zaposlene na određeno vreme ili lica angažovana po drugim osnovima, koji imaju pristup ili koriste mobilne uređaje u vlasništvu "Iron Mountain d.o.o.".

Rad na daljinu može se ostvariti i korišćenjem uređaja koji nisu mobilni na način definisan P-014-Kontrola pristupa resursima Ovi uređaji, pri tome, moraju imati primenjene najmanje iste bezbednosne mere kao i srodni uređaji koji se nalaze u okviru mreže, dok se za zaštitu komunikacije moraju primeniti iste mere kao i za zaštitu komunikacije mobilnih uređaja. Korisnici ovih uređaja moraju obezbediti dovoljno bezbedan prostor za njihov rad. Kontrolor kvaliteta odgovoran je za vođenje evidencije o svim uređajima namenjenim za rad na daljinu. Evidencija o uređajima treba da sadrži podatke koji su neophodni da bi se uređaj i/ili korisnik nedvosmisleno identifikovali, kao što su proizvođač, model, serijski broj, inventarski broj. Korisnik mobilnog uređaja u obavezi je da svaki bezbednosni incident prijavi "Glavnom administratoru bezbednosti" bez odlaganja, odmah po saznanju. da dostavi pisanu izjavu o okolnostima bezbednosnog incidenta. Pod pojmom bezbednosni incident se smatra krađa, gubitak mobilnog uređaja ili bilo koji drugi događaj koji dovodi do narušavanja tajnosti i integriteta podataka koji se nalaze na mobilnom uređaju. Glavni administrator bezbednosti je u obavezi da, po prijavi bezbednosnog incidenta, neodložno blokira nestalom mobilnom uređaju pristup informacionom sistemu i korisniku promeni kredencijale za pristup.

U slučaju da se pronađe mobilni uređaj čiji nestanak je prijavljen, izvršiće trajno brisanje kompletnog medijuma za smeštanje operativnog sistema, aplikacija i podataka i ponovnu instalaciju operativnog sistema i potrebnih aplikacija.

Obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji obavljaju i u potpunosti razumeju svoju odgovornost

Član 8.

"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).

Provera kandidata i uslovi zapošlavanja

“Iron Mountain d.o.o.” sprovodi postupke radi provere ispunjenosti uslova svakog pojedinačnog kandidata za zaposlenje, u skladu sa 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.

Obaveze u toku zaposlenja

Rukovodstvo "Iron Mountain d.o.o.” ima obavezu da zahteva od svih zaposlenih i radno angažovanih lica primenu mera zaštite bezbednosti, u skladu s ovim aktom i važećim procedurama.

"Iron Mountain d.o.o.” se posvećuje razvoju, implementaciji i održavanju sistema zaštite i bezbednosti podataka obezbeđujući uslove za integraciju kontrolnih mehanizama na sledeći način:

- Osigurava da se postupci zaštite sprovode na organizovan način i u skladu sa procedurama, održavajući kontinuitet;
- Štiti informacije i podatke sa sličnim profilom osetljivosti na jednaki način u svim organizacionim jedinicama;
- Sprovodi programe zaštite na dosledan i ujednačen način u svim organizacionim jedinicama;
- Koordinira bezbednost i zaštitu podataka u informacionom sistemu sa fizičkom zaštitom istih.

Zaposleni koji su odgovorni za nadzor, analizu, izveštavanje i preduzimanje aktivnosti u vezi sa sprovođenjem usvojene politike i procedura kontinuirano se usavršavaju radi unapređenja tehničkog i tehnološkog znanja. Glavni administrator bezbednosti je ovlašćen da preduzme hitne i neodložne mere u slučaju neposredne opasnosti po podatke i dokumentaciju koje su obuhvaćene merama zaštite.

Upoznavanje za bezbednošću informacija, sticanje znanja i obuka

Svi zaposleni u "Iron Mountain d.o.o." su dužni da prođu odgovarajuću obuku i redovno ažuriraju svoje znanje o procedurama koje regulišu bezbednost informacija, prilagođavajući je njihovim poslovnim zadacima i radnim mestima. Zaposleni redovno učestvuju u E-learning treninzima o informacionoj bezbednosti i zaštiti podataka.

Disciplinski postupak

Disciplinski postupak se sprovodi protiv zaposlenih koji su prekršili bezbednosne smernice ili na drugi način prekršili pravila i politiku koje važe i primenjuju se kod "Iron Mountain d.o.o.". Pokretanje disciplinskog postupka inicira se po predlogu rukovodioca, shodno Pravilniku o radu koji obuhvata posledice kršenja radne discipline.

Zaštita od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema

Član 9.

Zaposleni i druga angažovana lica, bez obzira na osnov angažovanja, imaju obavezu čuvanja poverljivih informacija od značaja za informacionu bezbednost IKT sistema i nakon prestanka ili promene radnog angažovanja. Dužnosti i odgovornosti koje ostaju relevantne i nakon završetka angažmana trebaju biti jasno definisane u tekstualnom delu ugovora o radu za zaposlene ili u uslovima angažovanja za osobe van radnog odnosa.

Ova mera je bliže određena:

- Procedurom o pravima pristupa informacionom sistemu
- Ugovorom o radu

- Ugovorom o angažovanju lica van radnog odnosa
- Sporazumom o poverljivosti

Oblasti HR/QA/IT se bave procedurama prilikom završetka radnog odnosa ili angažovanja, preduzimajući sledeće korake:

- Proverava ispunjenost svih uslova u vezi čuvanja i iznošenja podataka u elektronskom i papirnom formatu,
- Pregleda sve naloge i pristupe sistemu koji su bili dostupni zaposlenom, preuzima od zaposlenog elektronske i druge mobilne uređaje,
- Proverava vraćene mobilne uređaje i uređaje za prenošenje podataka,
- daje nalog za ukidanje naloga elektronske pošte i svih drugih prava pristupa sistemu "Iron Mountain d.o.o." na dan prestanka radnog odnosa ili drugog osnova angažovanja bivšeg zaposlenog,
- Pregleda sve naloge za pristup odlazećeg zaposlenog i prikuplja pristupne šifre i kodove radi ukidanja/promene istih na dan odlaska,
- Preuzima kartice ili druge uređaje kojima se omogućava pristup poslovnim prostorijama i opremi "Iron Mountain d.o.o.".
- Popunjava se Exit kontrolna lista kada se preduzimaju ove aktivnosti.

Identifikovanje informacionih dobara i određivanje odgovornosti na njihovu zaštitu

Član 10.

Informaciona dobra obuhvataju programske kodove, konfiguraciju hardverskih komponenti, operativnih sistema, tehničku i korisničku dokumentaciju, podatke u datotekama i bazama podataka, kao i unutrašnje opšte akte i procedure. Ovo je detaljnije opisano u dokumentu “Lista resursa”.

Popisivanje imovine

"Iron Mountain d.o.o." vrši identifikaciju imovine koja odgovara životnom ciklusu informacija i dokumentuje njen značaj. Životni ciklus informacija obuhvata kreiranje, obradu, skladištenje, prenos, brisanje i uništavanje podataka i informacija. "Iron Mountain d.o.o." pravi popis dobara koji je tačan, ažuran, konzistentan i usklađen sa Iron Mountain globalnom procedurom "Asset Management Policy/Asset Management Standard."

Evidenciju o informacionim dobrima, sredstvima i imovini za obradu informacionih dobara vodi "Interni revizor".

Vlasništvo nad imovinom, prihvatljivo korišćenje i njen povraćaj

Osobe koje su odgovorne za kontrolisanje životnog ciklusa imovine obavezne su da pravilno upravljaju imovinom tokom celog životnog ciklusa.

"Iron Mountain d.o.o." unutar internog akta o rukovanju imovinom, odnosno Asset Management Policy/Asset Management Standard, reguliše pravila za prihvatljivo korišćenje imovine povezane sa informacijama i opremom za obradu informacija.

Zaposleni i eksterni korisnici obavezni su da vrate svu imovinu "Iron Mountain d.o.o." koju poseduju nakon prestanka njihovog zaposlenja, ugovora ili sporazuma o angažovanju na određenim poslovima i zadacima.

Tokom otkaznog roka zaposlenih, "Iron Mountain d.o.o." kontroliše njihovo neovlašćeno kopiranje, umnožavanje ili preuzimanje relevantnih zaštićenih informacija.

Klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz Člana 3. Zakona o informacionoj bezbednosti

Član 11.

Klasifikacija podataka je proces utvrđivanja i pojedinačnog dodeljivanja nivoa tajnosti podataka, skladu sa njihovim značajem za "Iron Mountain d.o.o."

"Iron Mountain d.o.o." označava tipove i lokacije podataka kao poverljive, interne ili javne, kako je opisano u Proceduri P-015 Klasifikacija informacija. Imovina se obeležava pomoću identifikacionih nalepnica koje nose odgovarajuću klasifikacionu oznaku.

"Iron Mountain d.o.o." vrši klasifikaciju radi:

- Jačanja korisničke odgovornosti, kako bi korisnici mogli da uoče i prepoznaju poslovnu vrednost podataka prilikom čuvanja ili slanja, postajući svesni odgovornosti za neovlašćeno korišćenje ili prenošenje;
- Podizanja svesti o vrednosti informacija ili dokumenata;
- Zaštite podataka u pokretu radi bolje i inteligentnije integracije sa DLP, WEB gateway i ostalim proizvodima za zaštitu parametara i krajnjih uređaja;
- Zaštite sadržaja;
- Integracije sa sistemima za arhiviranje.

Klasifikacija dokumenata mora da bude usklađena sa pravilima kontrole pristupa.

"Iron Mountain d.o.o." postupa u skladu sa usvojenom Šemom klasifikovanja podataka. Posebnom procedurom se definišu radnje za postupanje, obradu, skladištenje i prenos podataka.

Procedura P-014 Kontrola pristupa resursima sadržava:

- Ograničenja pristupa koja podržavaju zahteve za zaštitu svakog nivoa klasifikacije;
- Održavanje zvaničnog zapisa o ovlašćenim primaocima imovine;
- Zaštitu privremenih ili trajnih kopija podataka na nivou koji je u skladu sa zaštitom originalne informacije;
- Skladištenje informacione imovine u skladu sa specifikacijama proizvođača;
- Jasno obeležavanje svih kopija medija na koje ovlašćeni primalac treba da obrati pažnju.

Zaštita nosača podataka

Član 12.

"Iron Mountain d.o.o." garantuje zaštitu od neovlašćenog otkrivanja, izmena, brisanja ili uništenja podataka smeštenih na nosačima podataka. Praćenje nosača podataka i zabeleženih informacija sprovodi Glavni administrator bezbednosti.

Upravljanje prenosnim nosačima podataka (medijuma)

“Iron Mountain d.o.o.” je dužan da razvija i implementira proceduru o upravljanju prenosnim nosačima, u skladu sa usvojenom Šemom klasifikovanja podataka.

Procedura upravljanja prenosnim nosačima može sadržavati sledeće odredbe:

- Sadržaj svakog medijuma koji se može ponovo koristiti i koji će se iznositi izvan organizacije, onda kada više nije potreban, se uništavaju, shodno proceduri.
- Za sve medijume koji se iznose iz organizacije, onda kada je to neophodno i izvodljivo, treba zahtevati odobrenje, a o svim takvim iznošenjima treba voditi evidenciju, kako bi se sačuvao trag za proveru.
- Sve medijume treba skladištiti na bezbednom i zaštićenom mestu, u skladu sa preporukama proizvođača.
- Korišćenje kriptografskih tehnika za zaštitu podataka na prenosnim medijumima, ako su poverljivost ili integritet podataka važni.
- Podaci treba da budu preneti na novi medijum pre nego što postanu nečitljivi.
- Višestruke kopije vrednih podataka treba čuvati na odvojenim medijumima kako bi se dodatno smanjio rizik od slučajnog oštećenja ili gubitka podataka.
- Da bi se ograničila mogućnost gubljenja podataka, treba predvideti registraciju prenosnih medijuma.
- Pokretne prenosne medije treba koristiti samo ako za to postoji poslovna potreba.
- Ukoliko postoji poslovna potreba za korišćenjem prenosnih medijuma, neophodno je pratiti prenos podataka na takve medijume.

Rashodovanje nosača podataka (medijuma)

Procedura upravljanja prenosnim nosačima može sadržavati sledeće odredbe:

- Sadržaj svakog medijuma koji se može ponovo koristiti i koji će se iznositi izvan organizacije, onda kada više nije potreban, se uništavaju, shodno proceduri.
- Za sve medijume koji se iznose iz organizacije, onda kada je to neophodno i izvodljivo, treba zahtevati odobrenje, a o svim takvim iznošenjima treba voditi evidenciju, kako bi se sačuvao trag za proveru.
- Sve medijume treba skladištiti na bezbednom i zaštićenom mestu, u skladu sa preporukama proizvođača.
- Korišćenje kriptografskih tehnika za zaštitu podataka na prenosnim medijumima, ako su poverljivost ili integritet podataka važni.
- Podaci treba da budu preneti na novi medijum pre nego što postanu nečitljivi.
- Višestruke kopije vrednih podataka treba čuvati na odvojenim medijumima kako bi se dodatno smanjio rizik od slučajnog oštećenja ili gubitka podataka.
- Da bi se ograničila mogućnost gubljenja podataka, treba predvideti registraciju prenosnih medijuma.
- Pokretne prenosne medije treba koristiti samo ako za to postoji poslovna potreba.
- Ukoliko postoji poslovna potreba za korišćenjem prenosnih medijuma, neophodno je pratiti prenos podataka na takve medijume.

Fizički prenos nosača podataka (medijuma)

Nosači podataka koji sadrže informacije se štite od neovlašćenog pristupa, zloupotrebe ili oštećenja tokom transporta. Kada poverljiva informacija na medijumu nije šifrovana, potrebno je dodatno fizički zaštititi medijum.

Smernice za bezbedan transport:

- Koristiti pouzdani transport ili kurire.
- Potrebno je uvesti proveru identiteta kurira.

- Karakteristike opreme za prenos moraju da budu takve da obezbede zaštitu od svih fizičkih oštećenja koja bi mogla nastati tokom transporta.

U slučaju transporta nosača podataka s informacijama, Generalni Direktor daje saglasnost i određuje lice koje će vršiti transport i način transporta.

Ograničenje pristupa podacima i sredstvima za obradu podataka

Član 13.

Podacima i sredstvima za obradu podataka neophodno je ograničiti pristup u skladu s utvrđenim stepenom tajnosti podataka i usvojenom procedurom klasifikacije podataka.

"Iron Mountain d.o.o." poseduje Kontrolnu listu pristupa koja sadrži popis svih informacionih objekata i subjekata koji im mogu pristupiti. Korisnicima je dozvoljen pristup samo mreži i mrežnim uslugama za čije korišćenje su ovlašćeni. Kotrola pristupa je definisana procedurom P-014 Kontrola pristupa resursima.

Operator IKT sistema "Iron Mountain d.o.o." će posebnim dokumentom urediti pristup mreži i mrežnim uređajima.

Sadržaj procedure o pristupu mreži i mrežnim uređajima obuhvata:

- Listu mreža i mrežnih usluga kojima je pristup dozvoljen.
- Načine autorizacije radi utvrđivanja kome je odobren pristup, kojoj mreži i kojim uslugama.
- Način upravljanja zaštitom pristupa mrežnim priključcima i uslugama.
- Sredstva koja se koriste za pristup mrežama i mrežnim uslugama.
- Zahteve u pogledu verifikacije korisnika za pristup različitim mrežnim uslugama.
- Načini nadgledanja korišćenja mrežnih usluga

Opšti uslovi od 28.04.2025. godine, primenjeni na ugovorni odnos između "Iron Mountain d.o.o." i Mainstream doo, 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.

Odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža

Član 14.

"Iron Mountain d.o.o." upravlja pristupom informaciono-komunikacionim tehnologijama (IKT) i uslugama putem korišćenja korisničkih identifikatora.

- Upravljanje korisničkim identifikatorima vrši se uz poštovanje sledećih principa:
- Korisnički identifikatori su jedinstveni, tako da se korisnici mogu vezati uz njih i učiniti odgovornim za svoje aktivnosti.
- Korišćenje zajedničkih identifikatora dozvoljava se samo kada je to pogodno za obavljanje posla uz prethodno odobrenje.
- Korisnicima kojima je prestao radni odnos ili period angažovanja trenutno se onemogućavaju ili uklanjaju korisnički identifikatori.
- Periodično identifikovanje i uklanjanje ili onemogućavanje višestrukih korisničkih identifikatora.
- Višestruki identifikatori nekog korisnika se ne izdaju drugim korisnicima.

Pravo pristupa informaciono-komunikacionom sistemu se dodeljuje svakom korisniku u skladu sa zadacima koje obavlja. Svaki korisnik poseduje jedinstvene podatke za prijavljivanje, uključujući jedinstvenu šifru, koja se ne sme deliti sa ostalim korisnicima.

Dodeljivanje privilegovanih (administratorskih) prava na pristup vrši se na osnovu odluke odgovornog lica.

Privilegovana prava na pristup dodeljuju se posebno za svaki sistemski objekat uz definisan rok trajanja tih prava.

Privilegovana prava na pristup koja treba dodeliti korisničkom identifikatoru su različita od onih koja se koriste za redovne aktivnosti. Redovne poslovne aktivnosti ne treba vršiti iz privilegovanih korisničkih identifikatora. Kompetencije korisnika sa privilegovanim pravima na pristup se redovno preispituju radi provere da li su u skladu sa njihovim obavezama.

Zabranjeno je neovlašćeno korišćenje opštih korisničkih identifikatora administratora.

Šifre za pristup opštim korisničkim identifikatorima administratora se menjaju promenom korisnika.

Operator IKT sistema jednom godišnje vrši preispitivanje prava korisnika na pristup, kao i nakon svake promene (unapređenje, razrešenje i kraj zaposlenja).

Zaposlenima, drugim radno angažovanim i eksternim korisnicima informacija i opreme za obradu informacija po prestanku zaposlenja ili isteku ugovora ukida se pravo na pristup.

Utvrđivanje odgovrnosti korisnika za zaštitu sopstvenih sredstava za autentifikaciju

Član 15.

Autentifikacija korisnika koji imaju odobren pristup sistemu obavlja se putem jedinstvenog korisničkog imena i lozinke.

Svi korisnici su obavezni da:

- Čuvaju korisničko ime i lozinku u tajnosti, ne otkrivaju ih drugim osobama, uključujući nadređene.
- Izbegavaju čuvanje korisničkog imena i lozinke u pisanoj formi.
- Menjaju lozinku čim primete bilo kakve naznake mogućeg ugrožavanja.

Lozinke moraju da ispunjavaju sledeće uslove:

- Sadrže najmanje 9 alfanumeričkih karaktera.
- Imaju najmanje jedno veliko i jedno malo slovo ili barem jedan od specijalnih znakova (~ ` ! @ # $ % ^ & * ( ) + . / \ ? _ ,).
- Imaju najmanje 1 broj (0-9).
- Ne smeju se zasnivati na ličnim podacima korisnika, kao što su ime, telefonski broj ili datum rođenja, i ne smeju sadržavati više od 3 uzastopna identična brojčana ili slovna znaka.

Korisnici su obavezni da promene privremene lozinke prilikom prvog prijavljivanja.

Predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka

Član 16.

Radi zaštite podataka, "Iron Mountain d.o.o." koristi Cryptographic Protection Policy (Global) i

sprovodi politiku upotrebe kriptografskih kontrola, implementirajući pritom mehanizme i sisteme upravljanja ključevima.

Kriptografska zaštita obezbeđuje:

- Autentifikaciju (identifikaciju korisnika i drugih sistemskih entiteta koji zahtevaju pristup ili odobrenje korisničkih radnji);
- Neporecivost (primenu kriptografskih tehnika, obično digitalnog potpisa, kako bi se dobila potvrda o izvršavanju ili neizvršavanju određene radnje od strane pojedinca).Ovaj pristup ima za cilj osigurati integritet i sigurnost podataka, pružajući pouzdanu zaštitu od neovlašćenog pristupa i manipulacije

Poverljivost se postiže primenom šifrovanja radi zaštite osetljivih ili kritičnih informacija koje se skladište ili prenose.Integritet podataka koji se prenose obezbeđuje se očuvanjem nepromenljivosti.

Postupak kriptografske kontrole obuhvata:

- Analizu i procenu potreba primene kriptografije u poslovnim procesima, uključujući opšte principe prema kojima bi poslovne informacije trebalo da se štite.
- Određivanje nivoa zaštite uzimajući u obzir tip algoritma za šifrovanje podataka, jačinu i kvalitet kriptografskog algoritma.
- Primenu šifrovanja za zaštitu osetljivih podataka prilikom prenosa putem mobilnih ili drugih medija, uređaja ili komunikacionih vodova.
- Upravljanje ključevima, uključujući zaštitu kriptografskih ključeva i postupak oporavka šifrovanih podataka u slučaju gubitka, kompromitovanja ili oštećenja ključeva.

Član 17.

"Iron Mountain d.o.o." je dužan da preduzme mere radi sprečavanja neovlašćenog fizičkog pristupa prostorijama u kojima se nalaze sredstva i dokumenti informaciono-komunikacionog sistema (IKT sistema), kao i sprečavanja oštećenja i ometanja informacija. "Iron Mountain d.o.o." ovo reguliše po P-014 Kontrola pristupa resursima proceduri.

Zona razdvajanja i uspostavljanje sistema i fizičke bezbednosti

Naša kompanija se vodi globalnim standardom - Facility Physical Security Standard - Records Information kompanije Iron Mountain.

Zona razdvajanja predstavlja fizički definisane oblasti ili prostorije u zgradi ili na lokaciji gde se nalazi oprema za obradu informacija. Ove zone imaju za cilj obezbeđivanje sigurnosti i integriteta opreme i podataka. Evo detaljnijeg objašnjenja:

Fizička Ispravnost:

- Zone razdvajanja trebaju biti fizički ispravne, što znači da ne smeju imati procene ili prostore u kojima bi neko lako mogao ući neovlašćeno.
- Spoljni krov, zidovi i podovi na toj lokaciji trebaju biti od čvrstog materijala.
- Sva spoljna vrata trebaju biti potpuno zaštićena od neovlašćenog pristupa pomoću kontrolnih mehanizama poput rešetki, alarma, brava itd.
- Vrata i prozori trebaju biti zaključani u svim situacijama kada su bez nadzora, a za prozore se treba razmotriti dodatna spoljna zaštita, posebno na prizemlju.

Kontrola Pristupa:

- Treba postaviti prijavnicu sa osobljem ili druga sredstva za kontrolu fizičkog pristupa do lokacije ili zgrade.
- Pristup lokacijama ili zgradama treba biti ograničen samo na ovlašćeno osoblje.

Požarna Vrata:

- Sva protivpožarna vrata u bezbednosnoj zoni razdvajanja trebaju imati alarmni uređaj, biti pod nadzorom i redovno ispitivana kako bi se postigao potreban nivo otpornosti u skladu s odgovarajućim regionalnim, nacionalnim i međunarodnim standardima.
- Trebaju funkcionisati u skladu s lokalnim protivpožarnim pravilima u vezi s osiguranjem od otkaza.
- Radi efikasnog nadzora nad svim spoljnim vratima i prozorima, potrebno je instalirati odgovarajuće protivprovalne alarmne sisteme u skladu s nacionalnim, regionalnim ili međunarodnim standardima. Oblasti bez prisustva osoblja trebaju biti neprekidno pod budnim okom alarma. Nadzor treba biti obezbeđen i za druge oblasti, kao što su prostorije sa računarima ili prostorije za komunikacije.

- Organizacije trebaju odvojiti fizički opremu za obradu informacija kojom upravljaju od one kojom upravljaju treća lica kako bi se osigurala integritet i bezbednost sistema. Ovo doprinosi efikasnom upravljanju informacijama i smanjenju rizika od neovlašćenog pristupa.

Kontrola fizičkog ulaska

Bezbednosne oblasti moraju biti zaštićene odgovarajućim kontrolama ulaska kako bi se osiguralo da samo ovlašćenim pojedincima bude dozvoljen pristup, u skladu sa smernicama procedure P-014 "Kontrola pristupa resursima".

Smernice za kontrolu fizičkog ulaska obuhvataju:

- Evidentiranje datuma i vremena ulaska i izlaska posetilaca, sa neprekidnim nadzorom svih posetilaca, osim ako njihov pristup nije prethodno odobren.
- Odobravanje pristupa samo za specifične, autorizovane svrhe, uz izdavanje uputstava o bezbednosnim zahtevima za oblast i postupcima u vanrednim situacijama.
- Pristup oblastima gde se obrađuju ili čuvaju poverljive informacije treba ograničiti samo na ovlašćene osobe primenom odgovarajućih kontrola pristupa, kao što su dvofaktorski mehanizmi za proveru autentičnosti, poput pristupnih kartica i tajnih ličnih identifikacionih brojeva (PIN).
- Potrebno je bezbedno održavati i nadgledati evidenciju ili elektronsku proveru svih pristupa.
- Od svih zaposlenih, ugovarača i trećih strana, kao i od svih posetilaca, zahtevati nošenje vidljive identifikacije i narediti osoblju obezbeđenja ukoliko primete posetioce bez pratilaca ili osobu bez vidljive identifikacije.
- Zaposlenima kod pružalaca usluga obezbeđenja treba dozvoliti ograničen pristup bezbednosnim oblastima ili opremi za obradu osetljivih podataka, uz mogućnost aktiviranja kad god je to potrebno. Ovakav pristup treba biti odobren i stalno nadgledan.
- Prava pristupa bezbednosnim oblastima treba redovno revidirati i ažurirati, a po potrebi i povući.

Zaštita kancelarija, prostorija, sredstava, kao i zaštita od pretnji eksternih faktora iz okruženja

"Iron Mountain d.o.o." sprovodi adekvatne mere kontrole pristupa kako bi osigurao fizičku sigurnost kancelarija, prostorija i opreme. Takođe, kroz bezbednu konfiguraciju, sprečava pristup ključnoj opremi s ciljem očuvanja povjerljivosti informacija i sprečavanja neovlašćenih aktivnosti izvan objekta. Planira i implementira mere fizičke zaštite kako bi se adekvatno odgovorilo na potencijalne pretnje poput prirodnih katastrofa, neprijateljskih napada ili nesreća.

Rad u sigurnosnim zonama

Sigurnosne zone su podvrgnute sledećim merama zaštite:

- Osoblje treba biti informisano o aktivnostima unutar sigurnosne zone.
- Rad bez nadzora u sigurnosnim zonama je strogo zabranjen.
- Neaktivne sigurnosne zone trebaju biti fizički zaključane, a njihova provera se redovno sprovodi.
- Unos fotografskih, video, audio ili drugih uređaja za snimanje nije dozvoljen bez prethodnog odobrenja od strane odgovornog lica.

Evidenciju o pristupu sigurnosnoj zoni održava Glavni administrator bezbednosti .

Zaštita od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem

Član 18.

Postavljanje i zaštita opreme

Oprema se postavlja i štiti na način kojim se smanjuje rizik od pretnji i opasnosti iz okoline, kao i mogućnost neovlašćenog pristupa.

Smernice za bezbednost opreme:

- Oprema se postavlja na mestu koje se može obezbediti od neovlašćenog pristupa.
- Oprema za obradu informacija koja služi za pristup i korišćenje osetljivih podataka postavlja se na mestima koja nisu vidljiva neovlašćenim osobama.
- Vrši se redovna kontrola sistema za obezbeđenje, alarma, protivpožarne zaštite, kao i instalacija za vodu, struju, gas, elektronske komunikacije.
- Prostorije sa opremom treba redovno čistiti od prašine.
- Zabranjeno je konzumiranje hrane i pića, kao i pušenje u blizini opreme za obradu informacija.
- Redovno se prate temperatura i vlažnost vazduha.
- Oprema mora biti zaštićena od atmosferskih padavina.
- Oprema u industrijskom okruženju se štiti primenom specijalnih metoda zaštite.

Službenik obezbeđenja shodno proceduri P-033 Održavanje opreme redovno prati uslove okoline, kao što su temperatura i vlažnost, koji bi mogli negativno uticati na rad opreme za obradu informacija.

Pomoćne funkcije za podršku

Oprema se štiti od prekida napajanja na sledeći način:

- Pomoćna oprema za napajanje održava se u skladu sa specifikacijama opreme proizvođača i propisima.
- Kapacitet pomoćne opreme redovno procenjuje.
- Redovno se pregleda i ispituje u pogledu ispravnog funkcionisanja, vrše se popravke kvarova.
- Obezbeđuje se višestruko napajanje sa različitih trasa.

Održavanje opreme

Oprema se održava kako bi se osigurala njena neprekidna raspoloživost i nepovredivost, i to na sledeći način:

- Oprema se održava u skladu sa preporučenim servisnim intervalima i prema specifikacijama koje je dao isporučilac.
- Popravke i servisiranje opreme obavlja samo osoblje ovlašćeno za održavanje.
- O svim sumnjivim ili stvarnim neispravnostima, kao i o celokupnom preventivnom i korektivnom održavanju čuvaju se zapisi.
- Osetljive informacije treba izbrisati iz opreme.
- Pre vraćanja opreme u rad nakon održavanja, potrebno je pregledati kako bi se proverilo da nije neovlašćeno korišćena ili oštećena.

Izmeštanje i premeštanje imovine

Oprema, informacije ili softver se izmeštaju samo uz odobrenje odgovornog lica, a tokom izmeštaja se primenjuju sledeća pravila:

- Treba da se odrede zaposleni i spoljni korisnici koji imaju ovlašćenje da odobre izmeštaj imovine.
- Treba da se postave vremenska ograničenja za izmeštaj opreme i da se proverava usklađenost prilikom povratka.
- Treba dokumentovati identitet i ulogu lica koja koriste ili postupaju sa imovinom prilikom premštanja, a ova dokumentacija treba da bude vraćena sa opremom, informacijama ili softverom.

Bezbednost izmeštene opreme i imovine

Izmeštenu opremu treba opremiti bezbednosnim mehanizmima zaštite, uzimajući u obzir različite rizike koji se mogu javiti prilikom rada van uobičajenih prostorija.

Bezbedno rashodovanje ili ponovono korišćenje opreme

Svi delovi opreme koji sadrže medijume za čuvanje podataka potrebno je verifikovati kako bi se osiguralo da su svi osetljivi podaci i licencirani softveri pre rasipanja ili ponovnog korišćenja bezbedno uklonjeni.

Bezbednost opreme korisnika bez nadzora

Korisnici treba da obezbede da oprema koja je bez nadzora ima odgovarajuću zaštitu, s ciljem onemogućavanja pristupa zaštićenim informacijama i podacima.

Ostavljanje osetljivih i poverljivih dokumenata i materijala

Sva osetljiva i poverljiva dokumenta i materijali moraju biti uklonjeni sa radne površine i odloženi na odgovarajuće mesto koje se zaključava, u periodu kada zaposleni nije prisutan na svom radnom mestu ili kada se dokumenta i materijali ne koriste.

Procedura čistog radnog stola:

1. Sve osetljive i poverljive informacije u štampanom ili elektronskom obliku zaposleni moraju odložiti na sigurno mesto na kraju radnog dana ili kada nisu prisutni na svom radnom mestu.
2. Računari moraju biti zaključani u odsustvu zaposlenog i isključeni na kraju radnog dana.
3. Ormari i fioke u kojima se čuvaju poverljivi podaci moraju biti zaključani kada se ne koriste, a ključevi ne smeju biti ostavljeni na pristupačnom mestu bez nadzora.
4. Laptopovi moraju biti vezani uz pomoć odgovarajuće opreme ili zaključani u fioci. Tableti i ostali prenosni uređaji moraju biti zaključani u fioci.
5. Šifre za pristup ne smeju biti napisane i ostavljene na pristupačnom mestu.
6. Štampani materijal koji sadrži osetljive informacije mora odmah biti preuzet sa štampača prilikom štampanja.
7. Materijal koji je namenjen za bacanje treba uništiti ili odložiti na mesto koje se zaključava, a koje je namenjeno za odlaganje takve vrste materijala.

Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 19.

U cilju obezbeđivanja ispravnog i bezbednog funkcionisanja sredstava za obradu podataka, definišu se procedure za rukovanje sredstvima, koje se odnose na otpočinjanje i završetak pristupa informacionom sistemu, pravljenje rezervnih kopija, održavanje opreme, rukovanje nosačima podataka, kontrolu pristupa u prostorije sa serverskom infrastrukturom, komunikacionom opremom i sistemima za skladištenje podataka, kao i u slučajevima izmeštanja delova IKT sistema. Usvajanje i primena radnih procedura.

"Iron Mountain d.o.o." uspostavlja radne procedure koje sadrže instrukcije za detaljno izvršenje sledećih poslova:

a) instalacija i konfiguracija sistema;

b) obrada i postupanje sa informacijama (automatski i manuelno);

v) izrada rezervnih kopija;

g) obrada zahteva za vremenski raspored aktivnosti;

d) izrada instrukcija za postupanje u slučaju greške ili u drugim vanrednim situacijama koje mogu da nastanu u toku izvršavanja posla, uključujući ograničenja u korišćenju sistemskih pomoćnih funkcija;

đ) utvrđivanje liste kontakata za podršku i eskalaciju (uključujući eksterne kontakte za podršku) u slučaju neočekivanih operativnih ili tehničkih poteškoća;

e) izrada instrukcija za upravljanje poverljivim podacima;

ž) procedure za ponovno pokretanje sistema i oporavak, koje se koriste u slučaju otkaza sistema;

z) upravljanje sistemskim zapisima (logovima);

i) procedure za nadgledanje.

Za usvajanje, izmene i dopune radnih procedura ovlašćen je quality assurance/generalni menadžer.

Upravljanje raspoloživim kapacitetima

Kontinuirano se nadgleda, prilagođava i projektuje upotreba resursa u skladu sa potrebnim kapacitetima kako bi se osigurala neophodna performansa sistema. Periodično se sprovode sledeće aktivnosti:

a) Odbijanje ili ograničavanje propusnog opsega usluga koje nisu kritične za poslovanje, ukoliko su resursi ograničeni;

b) Povlačenje iz upotrebe aplikacija, sistema, baza podataka ili okruženja;

c) Optimizacija serije procesa i rasporeda;

d) Brisanje zastarelih podataka.

Zaštita podataka i sredstava za obradu podataka od zlonamernog softvera

Član 20.

Zlonamerni softver obuhvata sve programe koji su stvoreni s namerom da otežaju rad ili oštete neki umreženi ili neumreženi računar. Zaštita od zlonamernog softvera se oslanja na softver za otkrivanje zlonamernog softvera i otklanjanje štete, na poznavanje informacione bezbednosti, kao i na odgovarajuće kontrole pristupa sistemu i upravljanje potrebnim i zahtevanim promenama.

Postupak kontrole i preduzimanje mere protiv zlonamernog softvera

"Iron Mountain d.o.o." kao deo globalne kompanije Iron Mountain određuje i primenjujekontrole otkrivanja, sprečavanja i oporavka radi zaštite od zlonamernog softvera.

Globalne procedure kojima se vodimo:
-Network Intrusion Detection and Prevention Systems Standard
-Network Security Management Policy

Sadržaj procedure o zaštiti od zlonamernog softvera:

- Formalna zabrana korišćenja neautorizovanih softvera;

- Implementacija kontrola koje sprečavaju ili otkrivaju korišćenje neovlašćenog softvera;
- Implementacija kontrola koje sprečavaju ili otkrivaju korišćenje poznatih ili sumnjivih kompromitovanih veb-sajtova;
- Uspostavljanje formalne politike radi zaštite od rizika povezanih sa dobijanjem datoteka i softvera od ili preko spoljnih mreža, ili na bilo kom drugom medijumu, ukazujući na to koje zaštitne mere treba preduzeti;
- Smanjenje ranjivosti koje može eksploatisati neprijateljski softver, npr. kroz upravljanje tehničkim ranjivostima;
- Sprovođenje redovnih preispitivanja softvera i sadržaja podataka u sistemima koji podržavaju kritične poslovne procese; prisustvo bilo kakvih neodobrenih datoteka ili neautorizovanih dopuna treba formalno istražiti;
- Instaliranje i redovno ažuriranje softvera za otkrivanje zlonamernog softvera i oporavak radi pretraživanja računara i medijuma kao kontrolu iz predostrožnosti, ili na rutinskoj osnovi.

Lista provera koja se sprovodi obuhvata:

a) Proveru, pre korišćenja, svih datoteka na elektronskim ili optičkim medijumima, kao i datoteka primljenih preko mreža, da li sadrže zlonamerni softver;

b) Proveru, pre korišćenja, sadržaja priloga elektronske pošte i preuzetih sadržaja, da li sadrže zlonamerni softver; ovu proveru treba sprovoditi na raznim mestima, npr. na serverima za elektronsku poštu, na stonim računarima ili prilikom ulaska u mrežu operatora IKT sistema;

v) Proveru postojanja zlonamernih softvera na veb-stranicama;

g) Definisanje procedura za menadžment i odgovornosti za postupanje sa zaštitom od zlonamernog softvera u sistemima, obuka za njihovo korišćenje, izveštavanje i oporavak od napada zlonamernim softverom;

d) Pripremu odgovarajućih planova za kontinuitet poslovanja prilikom oporavka od napada zlonamernim softverom, uključujući sve neophodne rezervne kopije podataka i softvera i mehanizme za oporavak;

đ) Implementaciju procedura za redovno prikupljanje informacija, kao što je pretplata na adresne listove za dostavu ili provera veb-stranica na kojima se daju informacije o novim zlonamernim softverima;

e) Implementaciju procedura za verifikaciju informacija o zlonamernim softverima i obezbeđenje da su upozoravajući izveštaji tačni i informativni; rukovodioci treba da osiguraju da se za razlikovanje lažnih od stvarnih zlonamernih softvera koriste kvalifikovani izvori, npr. provereni časopisi,

pouzdane stranice na Internet mreži ili isporučioci programa protiv zlonamernih softvera; svi korisnici treba da budu svesni problema pojave duhovitih ili zlonamernih obmana i onoga što treba da rade posle njihovog prijema.

Preporučuje se donošenje i procedure o antivirusnoj zaštiti i procedure o podizanju svesti zaposlenih o informacionoj bezbednosti.

U slučaju da korisnik primeti neobično ponašanje računara, zapazanje treba bez odlaganja da prijavi "Sistem administratoru".

U cilju zaštite od upada u IKT sistem, globalni IT tim je dužan da održava sistem za sprečavanje upada.

Korisnicima koji su priključeni na IKT sistem u slučaju dokažane zloupotrebe Glavni administrator bezbednosti / Sistem administrator može ukinuti pristup.

Zaštita od gubitka podataka
Član 21

"Iron Mountain d.o.o." sprovodi izradu rezervnih kopija koje obuhvataju sistemsku informaciju, aplikacije i podatke neophodne za obnovu celokupnog sistema u slučaju vanrednih okolnosti.

Rezervne kopije informacija i podataka

Redovno se prave i proveravaju rezervne kopije informacija, shodno globalnoj "Iron Mountain d.o.o." proceduri "Systems and Information Backup Policy", softvera i dupliciranih sistema. Zaštitne kopije omogućavaju korisnicima povraćaj podataka, funkcionalnost servisa i aplikacija nakon uništenja ili oštećenja izazvanih hakerskim napadima, hardverskim kvarovima, korisničkim greškama, prirodnim katastrofama i drugim nesrećama. Pojam zaštitnih kopija obuhvata kreiranje rezervnih kopija korisničkih podataka, konfiguracionih i log fajlova, ključnih fajlova za rad operativnih sistema (servera, korisničkih i komunikacionih) ili kompletnih operativnih sistema, aplikacija, servisa i baza podataka.

Zaštitne kopije trebaju omogućiti brzo i efikasno vraćanje sistema u funkciju u slučaju nepredviđenih događaja. Njih je preporučljivo praviti u periodima kada nije smanjena dostupnost servisa, aplikacija, baza podataka i komunikacionih kapaciteta IKT sistema.

Za čuvanje zaštitnih kopija koriste se hard diskovi, eksterni hard diskovi i CD/DVD mediji. Nadležna organizaciona jedinica za IT obavlja sledeće zadatke:

1. Procenjuje osetljive i kritične podatke za koje je potrebno praviti rezervne kopije.
2. Kreira plan pravljenja rezervnih kopija.
3. Pravi zaštitne kopije serverskog operativnog sistema i podataka, komunikacionog operativnog sistema i konfiguracionih fajlova, aplikacija, servisa i baza podataka.
4. Verifikuje uspešno pravljenje rezervnih kopija.
5. Vodi evidenciju urađenih rezervnih kopija.
6. Odlaže kopije na bezbedno mesto.
7. Testira ispravnost rezervnih kopija i procedura za pravljenje zaštitnih kopija.
8. Restaurira podatke sa rezervnih kopija.

Plan pravljenja rezervnih kopija informacija uključuje sledeće:

1. Precizno i potpuno dokumentovane zapise o rezervnim kopijama i postupcima obnavljanja.
2. Definisanje opsega i učestalosti izrade rezervnih kopija.
3. Rezervne kopije treba prilagoditi poslovnim potrebama organizacije, uz uzimanje u obzir kritičnosti tih informacija za kontinuitet poslovanja.
4. Neophodno je skladištiti ih na lokaciji dovoljno udaljenoj kako bi se izbegla mogućnost oštećenja na glavnoj lokaciji.
5. Medije sa rezervnim kopijama treba redovno proveravati, obezbeđujući sigurnost njihove upotrebe u vanrednim situacijama i kada je to potrebno.

6. U situacijama gde je povjerljivost od suštinskog značaja, rezervne kopije treba dodatno zaštiti šifrovanjem.

Sistem inženjer je odgovoran za zaštitu od gubitka podataka.

Čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema

Član 22.

U IKT sistemu kompanije "Iron Mountain d.o.o." evidentiraju se zapisi o događajima (logovi) koji se odnose na aktivnosti korisnika, greške i događaje vezane za informacionu bezbednost.

Dnevnici zapisa

"Iron Mountain d.o.o." vodi evidenciju o događajima, beležeći aktivnosti korisnika, greške i događaje vezane za informacionu bezbednost. Ovi zapisi se čuvaju i redovno pregledaju. Sistem administrator nema dozvolu da briše ili deaktivira dnevnike svojih aktivnosti.

Zapisi o događajima obuhvataju:

- Identifikatore korisnika;
- Aktivnosti sistema;
- Datume, vreme i detalje ključnih događaja, kao što su prijava i odjava;
- Zapise o uspešnim i neuspešnim pokušajima pristupa sistemu;
- Zapise o uspešnim i neuspešnim pokušajima pristupa podacima i drugim resursima;
- Promene u konfiguraciji sistema;
- Datoteke kojima se pristupalo i vrste pristupa;
- Mrežne adrese i protokole;
- Alarme koje je sistem za kontrolu pristupa aktivirao.

Zaštita informacija u zapisima

Sredstva za zapisivanje i zabeležene informacije su zaštićeni od neovlašćenog menjanja i pristupa. Zabranjeno je neovlašćeno unošenje sledećih izmena:

- Menjanje tipova poruka koje se zabeležavaju;
- Unošenje izmena u datoteke sa zapisima ili njihovo brisanje;
- Prepunjavanje medijuma za zapise, što dovodi do otkaza zapisivanja događaja ili upisivanja preko već ranije zabeleženog.

Zapisi administratora i operatora

Aktivnosti administratora i sistema se zapisuju, a zapisi štite i redovno preispituju. Vlasnici privilegovanih korisničkih naloga mogu biti u stanju da upravljaju zapisima na opremi za obradu informacija koja je pod njihovom direktnom kontrolom, na koji način se štite i pregledaju zapisi da bi se održala odgovornost za privilegovane korisnike.

Za čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema zadužen je Glavni administrator bezbednosti.

Obezbeđivanje integriteta softvera i operativnih sistema

Član 23.

"Iron Mountain d.o.o." sprovodi procedure kojima se obezbeđuje kontrola integriteta instaliranog softvera i operativnih sistema, u skladu sa smernicama za kontrolu promena i instalaciju softvera.

Smernice za kontrolu promena i instalaciju softvera obuhvataju:

- Ažuriranje operativnog softvera, aplikacija i programskih biblioteka koje mogu obavljati samo ovlašćeni administratori, nakon dobijanja odgovarajućeg ovlašćenja od rukovodioca.

- Operativni sistemi trebaju sadržavati samo odobrene izvršne kodove, a ne i razvojne kodove ili kompajlere.
- Aplikacije i operativni sistemski softver treba implementirati tek nakon obimnog i uspešno sprovedenog ispitivanja, koje obuhvata ispitivanje primenljivosti, bezbednosti, uticaja na druge sisteme i pogodnosti za korišćenje. Ispitivanja treba sprovoditi na zasebnim sistemima, odnosno testnim okruženjima.
- Potrebno je osigurati da su sve odgovarajuće biblioteke izvornih programa ažurirane.
- Pre implementacije bilo kakvih promena, treba uspostaviti strategiju povratka na prethodno stanje.
- Prilikom svih ažuriranja na bibliotekama operativnih programa, treba održavati zapise za proveru.
- Kao meru predostrožnosti za neočekivane situacije, treba sačuvati prethodne verzije aplikativnog softvera.
- Starije verzije softvera treba arhivirati zajedno sa svim potrebnim informacijama i parametrima, procedurama, detaljima konfiguracije i softverom za podršku, dok se podaci čuvaju u arhivi.

Sistemsku instalaciju i podešavanje softvera može obavljati isključivo sistemski administrator, odnosno zaposleni-korisnik koji ima odgovarajuća ovlašćenja za tu svrhu.

Zaštita od zloupotrebe tehničkih-bezbednosnih slabosti IKT sistema

Član 24.

"Iron Mountain d.o.o." sprovodi analizu IKT sistema radi utvrđivanja stepena izloženosti potencijalnim sigurnosnim slabostima. Nakon identifikacije tih slabosti, preduzimaju se odgovarajuće mere, uključujući njihovo otklanjanje ili primenu zaštitnih mera.

Upravljanje tehničkim ranjivostima

"Iron Mountain d.o.o." redovno prikuplja informacije o tehničkim ranjivostima informacionih sistema u upotrebi, procenjuje izloženost tim ranjivostima i preduzima odgovarajuće mere, uzimajući u obzir pripadajuće rizike.

Specifične informacije potrebne za podršku upravljanju tehničkim ranjivostima obuhvataju informacije o prodavcu softvera, verzije softvera, trenutno stanje rasporeda, kao i odgovorne osobe za taj softver.Smernice:

- "Iron Mountain d.o.o." definiše i uspostavlja uloge i odgovornosti u vezi sa upravljanjem tehničkim ranjivostima, uključujući nadzor, procenu rizika usled utvrđene ranjivosti, ispravke, praćenje imovine i sve odgovornosti za potrebna koordiniranja;
- Najmanje jednom mesečno, a po potrebi i češće, vrši analizu dnevnika aktivnosti (activity log, history, security log, transaction log itd.) radi identifikacije potencijalnih slabosti IKT sistema.
- Kada je moguća tehnička ranjivost identifikovana, identifikuju se pripadajući rizici i akcije koje treba preduzeti; takve akcije mogu obuhvatiti ispravke ranjivih sistema i/ili primenu drugih kontrola;
- Ako je ispravka dostupna od legitimnog izvora, tada se procenjuju rizici u vezi sa instaliranjem te ispravke (rizike koji nastaju usled ranjivosti treba uporediti sa rizikom vezanim za instaliranje ispravke);
- Ispravke se moraju prvo isprobati i vrednovati pre nego što se trajno ugrade, kako bi se osiguralo da će biti efikasne i da neće dovesti do sporednih uticaja koji se ne mogu tolerisati; ako ispravka nije dostupna, tada treba razmotriti druge kontrole, kao što su deaktiviranje usluga ili mogućnosti koje se odnose na ranjivost, prilagođavanje ili dodavanje kontrola pristupa (npr. zaštitna barijera na granicama mreže) ili pojačano nadgledanje kako bi se otkrili ili sprečili postojeći napadi i uticalo na povećanje svesti o ranjivosti;

- O svim preduzetim procedurama prave se zapisi za proveru, a proces upravljanja tehničkim ranjivostima treba redovno nadgledati i vrednovati kako bi se osigurala njegova efikasnost i efektivnost;
- Najpre se uzimaju u razmatranje sistemi sa visokim rizikom;
- Efikasan proces upravljanja tehničkim ranjivostima usklađuje se sa aktivnostima koje se odnose na upravljanje incidentima, tako da obezbedi tehničke procedure koje treba sprovesti ako se dogodi neki incident;
- Kreira se procedura koja uzima u obzir situaciju u kojoj je identifikovana ranjivost, ali ne postoji pogodna kontramera. U ovoj situaciji, organizacija treba da proceni rizik u odnosu na poznate ranjivosti i definiše odgovarajuće mere za otkrivanje, kao i korektivne mere.

Ukoliko se identifikuju ranjivosti koje mogu ugroziti bezbednost IKT sistema, "Global Information Security - Vulnerability Management Team" je dužan da odmah izvrši podešavanja, odnosno instalira softver koji će otkloniti uočene ranjivosti. Prvo se uzimaju u razmatranje sistemi sa visokim rizikom.

Ograničenja u pogledu instalacije softvera

Zabranjeno je instaliranje softvera na uređajima koji mogu dovesti do izloženosti IKT sistema bezbednosnim rizicima. "Iron Mountain d.o.o " dozvoljava samo ovlašćenim administratorima da instaliraju softver. Globalnim Iron Mountain standardom "Configuration Management Standard" je definisano koje vrste softvera zaposleni smeju da instaliraju, a koje su zabranjene.

Obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema

Član 25.

Tokom sprovođenja revizije IKT sistema, "Iron Mountain d.o.o." obezbeđuje da revizija ima što manji uticaj na funkcionisanje sistema. Postupak kontrole informacionih sistema obuhvata sledeće korake:

- Sa rukovodstvom su dogovoreni zahtevi za proveru pristupa sistemu i podacima.
- Predmet i područje ispitivanja za proveru unapred su dogovoreni i strogo kontrolisani.
- Ispitivanja za proveru su ograničena na pristup čitanjem.
- Pristup koji nije ograničen samo na čitanje treba dozvoliti samo za dobijanje izdvojenih kopija sistemskih datoteka koje se, nakon završene provere, brišu ili odgovarajuće štite ako postoji obaveza čuvanja takvih datoteka prema zahtevima za dokumentovanje provere.
- Zahtevi za posebnu ili dopunsku obradu moraju biti identifikovani, a o tome mora biti sačinjen pismeni sporazum.
- Ispitivanja za proveru mogu uticati na dostupnost sistema, pa se pokreću van radnog vremena.
- Sav pristup se nadgleda i beleži da bi se napravio referentni trag.

Planiranje i sprovođenje provere IKT sistema može vršiti isključivo "Glavni administrator bezbednosti", odnosno zaposleni-korisnik koji ima ovlašćenje za tu svrhu.

Bezbednost podataka koji se prenose unutar kompanije IKT sistema kao i izvan kompanija IKT sistema i lica van IKT sistema

Član 26.

Zaštita podataka koji se prenose komunikacionim sredstvima unutar "Iron Mountain d.o.o.", između operatora IKT sistema i lica van operatora IKT sistema, obezbeđuje se utvrđivanjem odgovarajućih pravila, procedura, potpisivanjem ugovora i sporazuma, kao i primenom adekvatnih kontrola.

- Pravila korišćenja elektronske pošte:

Upotreba elektronske pošte mora biti u skladu sa uspostavljenom globalnom procedurom Records and Information Management Email Policy i adekvatnom kontrolama nad sprovođenjem iste. Elektronska pošta se može koristiti isključivo za poslovne potrebe; razmena poruka ličnog sadržaja nije dozvoljena; svi podaci sadržani u porukama ili njihovom prilogu moraju biti u skladu sa standardima zaštite podataka.

- Pravila korišćenja Interneta:

Pristup sadržajima na Internetu je dozvoljen isključivo za poslovne namene. Na mreži je omogućeno nadgledanje, odnosno koristi se postupak periodične revizije i kontrolisanja logovanja, kako na prijemu tako i na slanju.

- Pravila korišćenja informacionih resursa:

Informacioni resursi se koriste isključivo u poslovne svrhe, na radu ili u vezi sa radom. Drugu namenu korišćenja posebno odobrava odgovorno lice, na obrazloženi pismeni zahtev korisnika.

Sporazumi o prenosu informacija

Bezbedan prenos poslovnih informacija između organizacije i trećeg lica obezbeđuje se poštovanjem sporazuma o prenosu informacija.

Sporazumi o prenosu informacija trebaju uključiti sledeće:

- Minimalne tehničke standarde za pakovanje i prenos informacija.
- Procedure za obezbeđenje sledljivosti i neporecivosti tokom prenosa informacija.
- Posebne kontrole koje se zahtevaju za zaštitu osetljivih detalja, uključujući primenu kriptografije.
- Održavanje lanca nadzora za informacije tokom celog procesa prenosa.
- Odgovornosti rukovodstva za kontrolu i izveštavanje o prenosu, otpremi i prijemu.
- Korišćenje dogovorenog sistema označavanja osetljivih ili kritičnih informacija, sa osiguranjem jasnog značenja oznaka i adekvatne zaštite tih informacija.
- Standarde za identifikovanje kurira koji učestvuju u prenosu.
- Obaveze i odgovornosti u slučaju incidenata koji mogu ugroziti bezbednost informacija, uključujući i gubitak podataka.

Razmena elektronskih poruka

Zaštita informacija uključenih u razmenu elektronskih poruka regulisana je Pprocedurom „P-017 - Pravilna upotreba informacionih resursa o bezbednosti u razmeni elektronskih poruka“. Procedura obuhvata:

- Zaštitu poruka od neovlašćenog pristupa, modifikovanja ili odbijanja usluga koje su u skladu sa klasifikacionom šemom koju je usvojio "Iron Mountain d.o.o.”.
- Obezbeđivanje ispravnog adresiranja i transporta poruka.
- Poštovanje zakonskih odredbi, na primer zahteva za elektronske potpise.
- Dobijanje odobrenja pre korišćenja javnih spoljnih usluga, kao što su razmena hitnih poruka, pristup i korišćenje društvenih mreža ili zajedničko korišćenje datoteka.

- Postavljanje strožih nivoa utvrđivanja verodostojnosti, kontrolisanjem pristupa iz mreža sa javnim pristupom.

Sporazumi o poverljivosti ili neotrkivanju

Sporazumi o poverljivosti ili neotkrivanju imaju za cilj zaštitu informacija "Iron Mountain d.o.o." i obavezuju potpisnike da informacije štite, koriste i objavljuju ih na odgovoran i autorizovan način. Da bi se identifikovali zahtevi za sporazumima o poverljivosti ili neotkrivanju, treba uzeti u obzir sledeće elemente:

- Definiciju informacija koje treba zaštititi.
- Očekivano trajanje sporazuma, uključujući slučajeve u kojima je potrebno da se poverljivost sačuva neograničeno.
- Postupanja koja se zahtevaju po isteku sporazuma, poput vraćanja ili uništavanja informacija.
- Dozvoljeno korišćenje poverljivih informacija i poslovnih tajni, kao i prava potpisnika da koriste informacije.
- Pravo na proveru i praćenje aktivnosti koje uključuju poverljive informacije.
- Proces za obaveštavanje i izveštavanje o neovlašćenom otkrivanju ili pristupu poverljivim informacijama.
- Radnje koje treba preduzeti u slučaju kršenja ovog sporazuma.

Obezbeđivanje aplikativnih usluga u javnim mrežama

Informacije obuhvaćene aplikativnim uslugama koje prolaze kroz javne mreže treba zaštititi od zloupotreba, neovlašćenog otkrivanja podataka i modifikacija. Neophodno je potvrditi identitet korisnika i izvršiti deljenje ovlašćenja i odgovornosti za postavljanje sadržaja, elektronskog potpisivanja ili obavljanje transakcija.

Zaštita transakcija aplikativnih usluga

Informacije uključene u transakcije aplikativnih usluga se štite da bi se sprečio nepotpun prenos, pogrešno usmeravanje, neovlašćeno menjanje poruka, neovlašćeno razotkrivanje, neovlašćeno kopiranje poruka ili ponovno emitovanje.

Transakcije moraju da podrže sledeće uslove:

- Strane koje učestvuju u transakciji moraju da primene elektronski potpis.
- Na komunikacionim kanalima primenjeno šifrovanje.
- Bezbednost protokola koji se koriste u transakcijama.

Zaštita sredstava operatora IKT sistema koja su dostupna pružaocima usluga

Član 29.

Politika bezbednosti razmene informacija u poslovnim odnosima sa pružaocima usluga i između nezavisnih pružalaca usluga

Ugovori koji se zaključuju sa pružaocima usluga koji imaju pristup informacijama, sredstvima ili opremi za obradu informacija "Iron Mountain d.o.o.", moraju sadržavati ugovornu odredbu o zaštiti i čuvanju poverljivosti informacija, podataka i dokumentacije - Ugovor o čuvanju poverljivih informacija (NDA). Pružaoci usluga imaju pravo na pristup informacijama koje su krajnje neophodne za pružanje predmetne usluge koja je ugovorena sa "Iron Mountain d.o.o.".

"Iron Mountain d.o.o." uspostavlja kontrolu bezbednosti informacija koje se odnose na procese i procedure koje će sprovoditi pružaoci usluga:

- Identifikovanje i dokumentovanje vrste pružaoca usluga kojima će "Iron Mountain d.o.o." dozvoliti pristup informacijama.
- Standardizovan proces za upravljanje odnosima između pružaoca usluga.
- Definisanje vrsta informacija kojima će različitim tipovima pružalaca usluga biti dozvoljeno radi pristupa, praćenja i kontrole pristupa.
- Minimalni zahtevi za bezbednost informacija za svaku vrstu informacija i vrstu pristupa.
- Procesi i procedure za praćenje pridržavanja utvrđenih zahteva za bezbednost za svaku vrstu dobavljača i vrstu pristupa.
- Kontrole za osiguranje integriteta informacija ili obrade informacija koje obezbeđuje bilo koja strana.
- Postupanje sa incidentima i nepredviđenim situacijama koje su u vezi sa pristupom pružalaca usluga, uključujući odgovornosti i organizaciju i pružaoce usluga.
- Upravljanje neophodnim promenama informacija, opreme za obradu informacija i svega ostalog što treba da se premesti i osiguranje da se bezbednost informacija održava tokom prelaznog perioda.

Ugovaranje obaveze obezbeđivanja bezbednosti u sporazumima sa pružaocima usluga

Pre nego što započne pregovore, potencijalni pružalac usluga obavezan je potpisati izjavu o poverljivosti i zaštiti podataka, informacija i dokumentacije. Ova izjava sadrži obavezu pružaoca usluga da informacije i podaci koje su dostavljeni ili na drugi način postali dostupni mogu biti korišćeni isključivo na način koji je prethodno odobren od strane "Iron Mountain d.o.o.", i to samo u svrhu izvršenja predmeta pregovora.

Izjava o poverljivosti, odnosno ugovor o pružanju usluga, mora sadržavati odredbu o poverljivosti sa jasno definisanom obavezom i odgovornošću pružaoca usluge, uz pretnju raskida ugovora i naknade štete u korist "Iron Mountain d.o.o." u slučaju povrede ove odredbe.

Posebne obaveze primaoca informacija obuhvataju:

- Čuvanje poverljivih informacija sa pažnjom jednakošću kao i vlastite poverljive informacije.

- Korišćenje poverljivih informacija samo u svrhu saradnje, posebno bez upotrebe komercijalnih informacija u komercijalne svrhe.
- Ne kopiranje, reprodukovanje ili beleženje poverljivih podataka, osim u navedene svrhe, uz označavanje i osiguravanje svih kopija oznakom poverljivosti.
- Očuvanje svih oznaka poverljivosti na informacijama i sprečavanje njihovog skrivanja, brisanja, uništavanja ili činjenja nečitljivim.
- Obaveštavanje davaoca informacija odmah ako dođe do povrede poverljivosti ovih informacija.
- Osiguranje da su svi ovlašćeni subjekti pod obavezom čuvanja i neotkrivanja poverljivih informacija, prema definiciji ovog ugovora, i snositi odgovornost za sve povrede ugovorne obaveze o poverljivosti.

Ugovorne strane se posebno obaveziju da postupaju obazrivo sa podacima o ličnosti do kojih mogu doći u postupku izvršenja usluga za operatora IKT sistema. Takođe, obavezuju se da te podatke čuvaju i postupaju u skladu sa propisima koji uređuju zaštitu podataka o ličnosti. U slučaju povrede ove obaveze, ugovorna strana čiji su podaci korišćeni ima pravo na raskid ugovora i pravo da zahteva naknadu štete usled neovlašćenog korišćenja podataka i informacija druge strane.

Pružaoci usluga dužni su da zahteve "Iron Mountain d.o.o." u vezi sa bezbednošću informacija prošire i na svoje podugovarače za dodatne usluge ili proizvode. Glavni administrator bezbednosti je odgovoran za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi pravilnika kojima su takve aktivnosti definisane.

Održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga
Član 30.

U cilju održavanja i obezbeđivanja ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga, "Iron Mountain d.o.o." uspostavlja mere nadzora i zaštite tokom pružanja usluga i nakon izvršenog posla.

Praćenje i preispitivanje izvršenja ugovorenih obaveza pružaoca usluga

Glavni administrator bezbednosti redovno prati, analizira, preispituje i proverava izvršene usluge i usaglašenost sa ugovorenim uslovima na sledeći način:

- Nadgledanje i preispitivanje usluga se može vršiti preko trećeg lica;
- Neophodno je poštovanje svih uslova iz sporazuma u vezi sa bezbednošću informacija, kao i sprečavanje svih incidenata i problema narušavanja bezbednosti, te omogućavanje upravljanja na odgovarajući način;
- Vrši se ocena kvaliteta izvršenja i saobraznosti ugovorene usluge;
- Pružalac usluge ima ugovornu obavezu da organizuje i pripremi periodične sastanke koji će obezbediti redovno izveštavanje "Operatora IKT sistema Iron Mountain" i unaprediti kvalitet ugovorenih usluga, odnosno umanjiti potencijalnu štetu ili incidente koji mogu nastati u postupku izvršenja usluge ili nakon početka primene;
- Glavni administrator bezbednosti održava potpunu kontrolu nad sprovođenjem usluga i osigurava uvid u sve osetljive ili kritične bezbednosne informacije i druga sredstva za obradu informacija kojima treća strana pristupa, koje procesuira ili kojima upravlja. Takođe održava uvid u bezbednosne aktivnosti kroz jasno definisan proces izveštavanja;
- Preispituje tragove provere i zapisa o događajima u vezi sa bezbednošću kod pružalaca usluga, odnosno operativnim problemima, otkazima, praćenju neispravnosti i smetnjama u vezi sa isporučenim uslugama.

Prilikom zaključenja ugovora neophodno je jasno definisati kvalitativne, operativne i finansijske kriterijume ocene; utvrditi postupak izveštavanja, praćenja i postupanja u skladu sa zahtevima "Operatora IKT sistema Iron Mountain" u postupku izvršenja ugovorenih usluga i izvršiti ocenu izvršenih usluga i kvaliteta pružaoca usluga.

Prilikom nadzora nad izvršenjem kvaliteta i saobraznosti ugovorene usluge proverava se da li pružalac usluge zadovoljava sve kriterijume koji su bili od presudnog značaja prilikom izbora, uključujući obim i kvalitet usluge, kao i da se u toku postupka izvršenja usluge može uticati na poboljšanje kvaliteta usluge ili načina i obima izvršenja, u skladu sa utvrđenim stvarnim potrebama "Operatora IKT sistema Iron Mountain".

U postupku objektivne evaluacije kvaliteta i obima pružene usluge u odnosu na ugovorenu, potrebno je prikupiti sve relevantne činjenice, podatke i dokumentaciju u vezi sa izvršenjem usluge, kao i prikupiti podatke od neposrednih, krajnjih, korisnika u vezi sa predmetom usluge. Evaluacija se može izvršiti slanjem upitnika, razgovorom sa izabranim pojedincima ili na osnovu anonimnog ankentiranja putem elektronske pošte.

Upravljanje promenama ugovorenih usluga od pružaoca usluga

Ugovorom sa pružaocem usluga treba obezbediti mogućnost kontinuiranog upravljanja promenama ugovorenih usluga, uključujući održavanje i unapređenje postojećih procedura i kontrolu bezbednosti informacija.

Promene koje se uzimaju u obzir su promene u sporazumima sa pružaocima usluga, povećanje obima tekućih usluga koje se nude, kao i promene koje uvodi "Operator IKT sistema Iron Mountain" radi implementacije nove ili promenjene aplikacije, sistema, kontrola ili procedura u cilju poboljšanja bezbednosti.

Prevencija i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama

Član 31.

Odgovornost pojedinaca i postupak odgovora na incidente

Posebnom globalnom Iron Mountain procedurom "Upravljanje incidentima P-025" se uređuje način odgovora na incidente narušavanja informacione bezbednosti i određuje osoba ovlašćena za kontakt u slučajevima narušavanja bezbednosti, kao i kontakt sa nadležnim organima.

Potrebne procedure

- Procedure za pripremu i planiranje odgovora na incidente, "Upravljanje incidentima P-025";
- Procedure za nadgledanje, detekciju, analizu i izveštavanje o događajima i incidentima u vezi sa bezbednošću informacija;
- Procedure za zapisivanje aktivnosti u okviru upravljanja incidentima;
- Procedure za postupanje sa sudskim dokazima;
- Procedure za ocenjivanje i odlučivanje o događajima u okviru bezbednosti informacija i ocenjivanje slabosti u pogledu bezbednosti informacija;

"Iron Mountain d.o.o." određuje Službenika bezbednosti i Sistem administratora, čiji je zadatak da pridržavajući se procedura određenih ovim članom, planiraju, detektuju, analiziraju i informišu nadležne tokom i nakon incidenta. Navedeni administratori moraju imati odgovarajuća tehnička znanja kako bi na najbrži i odgovarajući način mogli odgovoriti na bezbednosne incidente.

Službenik bezbednosti, u cilju prevencije od bezbednosnih rizika, obezbeđuje više (različitih i drugačijih) mehanizama za komunikaciju i koordinaciju u slučaju narušavanja bezbednosti.

Ovi mehanizmi mogu biti: obezbeđivanje kontaktnih informacija (broj telefona, elektronska adresa) pojedinaca i članova tima u okviru organizacije i van nje, sistem za praćenje problema, šifrovani

softver koji bi bio korišćen od strane pojedinaca u okviru organizacije i spoljnih stranaka, posebnu osiguranu prostoriju za čuvanje podataka i skladištenje poverljivog materijala.

U slučaju bilo kakvog incidenta koji može ugroziti bezbednost resursa IKT sistema, zaposleni koji to uoči dužan je da o tome odmah obavesti Službenika bezbednosti /Sistem administratora.

Izveštavanje o događajima u vezi sa bezbednošću informacija

Svi zaposleni moraju biti upoznati s obavezom i procedurom izveštavanja o događajima u vezi s informacionom bezbednošću. Službenik bezbednosti je dužan da pripremi plan i nekoliko metoda komunikacije koje bi mogle da se primene u zavisnosti od incidenta (elektronska pošta, veb sajtovi - interni, eksterni, portali, telefonska komunikacija, govorna poruka, pismeno izveštavanje, direktan kontakt).

U slučaju pogrešnog funkcionisanja ili drugih anomalija u radu sistema vrši se isto izveštavanje kao i u slučaju događaja u vezi s informacionom bezbednošću.

Procedura "Upravljanje incidentima P-025" reguliše:

- Zaposleni koji smatra da je došlo do napada ili zloupotrebe podataka mora odmah pripremiti opis problema i poslati ga elektronskom poštom sektoru za informacione tehnologije (help desk)/pozvati broj/prijaviti problem putem Internet strane za help desk;
- Adresu elektronske pošte, broj telefona i Internet stranu za help desk proverava sistem administrator; Sistem administrator vrši proveru prijavljenog incidenta i dalje postupa po odgovarajućoj proceduri.
- Kada je identifikovan incident, zaposleni je dužan da odmah obavesti Glavnog administratora bezbednosti i preduzme mere u cilju zaštite resursa IKT sistema. Glavni administrator bezbednosti vodi evidenciju o svim incidentima, kao i prijavama incidenata, u skladu s uredbom, na osnovu koje, protiv odgovornog lica, mogu da se vode disciplinski, prekršajni ili krivični postupci.

Izveštavanje o utvrđenim slabostima sistema zaštite

Svi zaposleni su u obavezi da o uočenim i utvrđenim slabostima IKT sistema izveste Glavnog administratora bezbednosti, u što kraćem roku, kako bi se incidenti ugrožavanja informacione bezbednosti sprečili i sprečio nastanak štete.

Odgovorno lice za obaveštavanje nadležnih organa o incidentima u IKT sistemu koji mogu imati značajan uticaj na ugrožavanje informacione bezbednosti postupa u skladu s odgovarajućom procedurom.

Događaji u vezi s informacionom bezbednošću se ocenjuju, i u skladu s analizom donosi se odluka da li je potrebno da se klasifikuju kao incidenti ugrožavanja informacione bezbednosti.

Odgovor na incidente narušavanja informacione bezbednosti

"Iron Mountain d.o.o." je u obavezi da usvoji Plan za prevenciju od bezbednosnih rizika. Plan za prevenciju od bezbednosnih rizika sadrži odgovore na pitanja ko treba da bude kontaktiran, kada i kako i koje akcije treba preduzeti momentalno u slučaju određenog napada?

Klasifikaciona šema – detalji o podacima koji se nalaze u sistemu, njihov nivo osetljivosti i poverljivosti.

Lista usluga – popis svih usluga koje "Iron Mountain d.o.o." pruža, rangirane po važnosti.

Plan za backup i restore podataka – definiše za koje podatke se radi backup, nosače podataka na koje će se snimati, gde se nosači čuvaju i koliko često se backup izvodi. Definiše i postupak za restore podataka.

Plan za zamenu opreme: Sadrži spisak potrebne opreme, rangiran po važnosti.

Odnosi sa javnošću: Utvrđena je odgovorna osoba zadužena za odnose sa javnošću, kao i uputstvo koje informacije je dozvoljeno javno objaviti u slučaju napada. Prikupljeno znanje iz analize i rešavanja incidenata koji su narušili informacionu bezbednost, "Iron Mountain d.o.o." koristi da bi identifikovala incidente koji se ponavljaju i smanjila verovatnoću i uticaj budućih incidenata.

Prikupljeno znanje iz analize i rešavanja incidenata koji su narušili informacionu bezbednost, "Iron Mountain d.o.o." koristi da bi se identifikovali incidenti koji se ponavljaju i smanjila verovatnoća i uticaj budućih incidenata.

Prikupljanje dokaza

"Iron Mountain d.o.o." definiše i primenjuje procedure za identifikaciju, sakupljanje, nabavku i čuvanje informacija koje mogu da služe kao dokazi u slučaju pokretanja disciplinskog, prekršajnog ili krivičnog postupka.

Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima
Član 32.

"Iron Mountain d.o.o." primenjuje mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima, kako bi IKT sistem u što kraćem roku bio u funkcionalnom stanju.

Planiranje kontinuiteta mera bezbednosti informacija

Kontinuitet poslovanja se osigurava kroz Plan za obezbeđenje kontinuiteta poslovanja i Plan oporavka od neželjenih događaja IKT sistema. Pri izradi Plana za obezbeđenje kontinuiteta poslovanja za hardverske komponente IKT sistema treba obuhvatiti sledeće:

- dokumentaciju za logički i fizički dijagram i kopije projekata;
- zaštitne kopije konfiguracionih fajlova i operativnog sistema aktivnih uređaja;
- postojanje rezervne opreme;
- unapred napravljene konfiguracije za različite scenarije;
- izradu rezervnih kopija.

Pri izradi Plana oporavka od neželjenih događaja IKT sistema:

- proceniti najkritičnije aplikacije, podatke, konfiguracione fajlove i sistemski softver za koji treba napraviti rezervne kopije;
- odrediti mesto čuvanja kopije;
- odrediti novu lokaciju rada IKT sistema u slučaju nemogućnosti rada na osnovnoj lokaciji/izbor računara koji će privremeno zameniti server dok se server ne stavi u funkciju.;
- navesti podatke o timu koji će biti angažovan na otklanjanju posledica neželjenih događaja;
- odrediti izvore neprekidnog napajanja električnom energijom.

Takođe, pri izradi Plana oporavka od neželjenih događaja IKT sistema potrebno je predvideti:

- postojanje dokumentacije za servise, aplikacije i baze podataka;
- procedure instalacije i konfigurisanja servisa, aplikacija i baza podataka;
- mesto čuvanja instalacija servisa, aplikacija i baza podataka i rezervne kopije podataka;
- podatke o timu koji će biti angažovan na otklanjanju posledica neželjenih događaja;

Implementacija kontinuiteta bezbednosti informacija

U slučaju vanrednih situacija, Glavni administrator bezbednosti primenjuje procedure i kontrole koje su deo Plana za obezbeđenje kontinuiteta poslovanja. Ovaj plan ima za cilj osiguravanje neophodnog nivoa kontinuiteta bezbednosti informacija, obezbeđujući funkcionisanje sistema i zaštitu informacija tokom kritičnih perioda. Glavni administrator bezbednosti redovno proverava usvojene procedure i kontrole kontinuiteta bezbednosti informacija.

Ova provera uključuje sledeće aspekte:

Vežbanje i Ispitivanje:

- Redovno vežbanje i simulacije različitih scenarija vanrednih situacija.
- Ispitivanje znanja i rutine zaposlenih u radu sa procesima i kontrolama bezbednosti informacija.
- Preispitivanje Efektivnosti Mera:

IRON MOUNTAIN®

- Aktivno preispitivanje efektivnosti usvojenih mera bezbednosti informacija.
- Pracenje i analiza promena u informacionim sistemima, procesima, procedurama kontrolama.

Obnova i Usavrsavanje:

- Proces obnove planova i procedura na osnovu dobijenih iskustava i novih informacija o bezbednosti.
- Usavrsavanje procesa i kontrola kako bi se povecala njihova adekvatnost i efikasnost.

Ove aktivnosti obezbeduju da kontinuitet bezbednosti informacija ostane na visokom nivou usred vanrednih okolnosti i da organizacija uspesno odgovori na potencijalne pretnje i rizike.

PRELAZNE I ZAVRSNE ODREDBE

Posebna obaveza Iron Mountain d.o.o

Clan 33.

Obaveza "Iron Mountain d.o.o." je da najmanje jednom godisnje izvrsi proveru IKT sistema i izvrsi eventualne izmene Akta o bezbednosti, u cilju provere adekvatnosti predvidenih mera zastite, kao i utvrdenih procedura, ovlascenja i odgovornosti u IKT sistemu Operatora IKT sistema. Stupanje na snagu Akta o bezbednosti

Clan 34.

Ovaj Akt o bezbednosti stupa na snagu 15.11.2023.

IRON MOUNTAIN doo

ODGOVORNO LICE