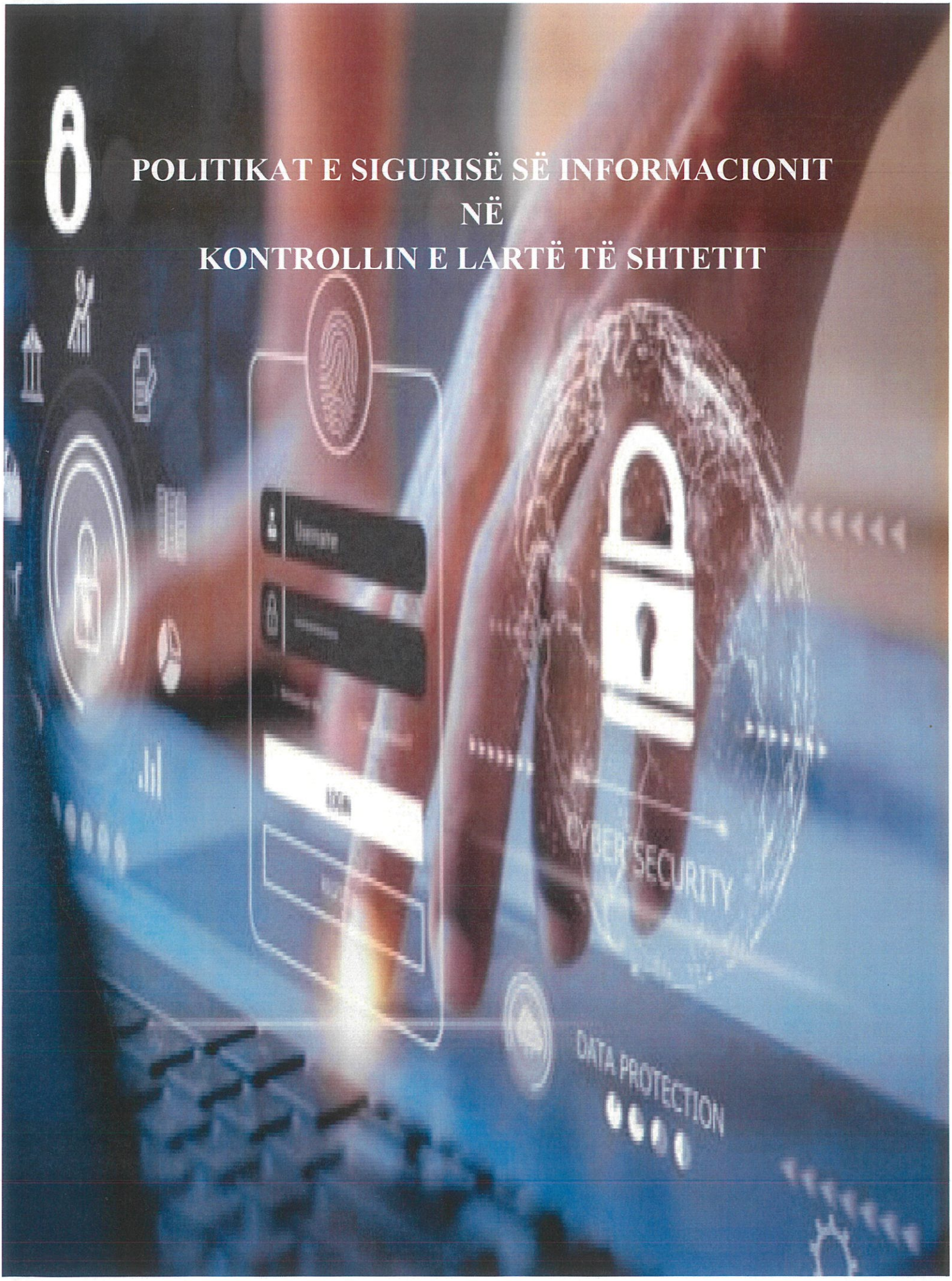
POLITIKAT E SIGURISË SË INFORMACIONIT NË KONTROLLIN E LARTË TË SHTETIT



1. Përmbajtja

Hyrja
Objektivat e Sigurisë së Informacionit
Përgjegjësitë
Menaxhimi i rrezikut të sigurisë së informacionit
Menaxhimi i aseteve
Kontrolli i aksesit
Siguria fizike dhe ambientale
Menaxhimi i komunikimeve dhe operacioneve
Siguria në rrjet
Blerja, zhvillimi dhe mirëmbajtja e sistemeve
Kontrolli i furnitorëve dhe palëve të treta
Menaxhimi i incidentit të sigurisë së informacionit
Mcnaxhimi i vazhdimësisë së institiucionit
Përputhshmëria me ligjet dhe rregulloret
Trajnimi dhe ndërgjegjësimi për sigurinë
Auditimi i brendshëm i sigurisë
Përmirësimi i vazhdueshëm
Detyrimi dhe pasojat disiplinore
Referenca

2. Hyrja

Qëllimi: Ky dokument ka për qëllim të përcaktojë politikat dhe masat e sigurisë që Kontrolli i Lartë i Shtetit do të ndjekë për të mbrojtur informacionin dhe sistemet e tij.
Ky dokument është hartuar në përputhje me standardin ISO/IEC 27001:2022, i cili përshkruan kërkesat për krijimin, zbatimin, mirëmbajtjen dhe përmirësimin e vazhdueshëm të një Sistemi të Menaxhimit të Sigurisë së Informacionit (SMSI).

Fusha e Zbatimit: Politikat e sigurisë së informacionit zbatohen për dhe nga të gjithë punonjësit, kontraktorët, partnerët dhe palët e treta që kanë akses në informacionet dhe sistemet informatike që disponon dhe akseson KLSH. Ato përfshijnë të gjitha aktivitetet që ndodhin në mjedisin e brendshëm të institucionit si dhe nëpërmjet sistemeve të jashtme të palëve të treta.

3. Objektivat e Sigurisë së Informacionit

Objektivat kryesore të kësaj politike për sigurinë e informacionit përfshijnë:

- **Konfidencialitetin** e informacionit, duke siguruar që vetëm individët e autorizuar të kenë qasje në të dhënat e caktuara;
- **Integritetin** e informacionit, duke mbrojtur të dhënat nga ndryshimet e paautorizuara;
- **Disponueshmërinë** e informacionit për personat e autorizuar kur të jetë e nevojshme.

Në:

- Të gjitha sistemet desktop, serverët, pajisjet e ruajtjes së të dhënave, sistemet e komunikimit, firewall-et, router-at, switch-at dhe cdo pajisje teknologjike që është në pronësinë e KLSH-ës;
- Të gjitha platformat IT, software-ët e sistemeve operative dhe aplikacionet e përdorura nga KLSH;
- Të gjitha të dhënat, informacionet, dokumentet, bazat e të dhënave, ose burimet e tjera të informacionit të ruajtura në KLSH.

4. Përgjegjësitë

Rolet dhe përgjegjësitë në KLSH janë përcaktuar dhe detajuar në tabelën e mëposhtme:

Pozicioni	Përgjegjësitë
Kryetari	• Miraton Strategjinë Institucionale, Strategjinë e IT, Politikat e Sigurisë së Informacionit si dhe Rregulloret dhe Procedurat në zbatim të tyre. • Prioritarizon investimet dhe sigurohet që po kryhen për mbështetjen e objektivave të institucionit. • Aprovon Iniciativat / Projektet InfoSec,
Sektretari i Përgjithshëm	• Monitoron implementimin e investimeve të miratuara në drejtim të teknologjisë së informacionit dhe sigurohet për përputhshmërinë me aktet ligjore dhe nënligjore në fuqi • Menaxhon buxhetin përkatës.
Koordinatori i Sigurisë së Informacionit / CISO	• Drejton ekipin e Sigurisë së Informacionit, duke përputhur nismat e Sigurisë së Informacionit me objektivat e institucionit. • Jep udhëzime në politikat e sigurisë dhe investimet që i mbrojnë ato. • Zhvillon dhe zbaton strategjinë / politikat e Sigurisë së Informacionit; • Shërben si pika e kontaktit për subjektet e të dhënave dhe autoritetet rregullatore.
Drejtoria e Teknologjisë së Informacionit	• Menaxhon operacionet e përditshme të sigurisë brenda insttiucionit; • Zbaton dhe ndjek politikat, standardet dhe procedurat e sigurisë. • Përgatit raporte të detajuara mbi gjendjen e sigurisë dhe incidentet. • Trajton incidentet e sigurisë dhe përpjekjet për reagim. • Mbikëqyr operacionet e Sigurisë së Informacionit dhe raporton te drejtuesit e KLSH-së; • Mirëmban dhe përditëson mjetet dhe teknologjitë e sigurisë. • Harton dhe zbaton zgjidhje dhe infrastrukturë të fuqishme sigurie. • Siguron përputhshmërinë me ligjet dhe rregulloret. • Zbaton dhe menaxhon enkriptimin, fireëall-et dhe masa të tjera të sigurisë. • Bashkëpunon me ekipet e IT dhe zhvillimit për të integruar masat e sigurisë. • Reagon dhe lehtëson incidentet e sigurisë, duke siguruar ndërprerje minimale. • Menaxhon kontrollin dhe autorizimin e qasjes së përdoruesve. • Mirëmban konfigurimet e sigurisë së sistemeve dhe aplikacioneve. • Monitoron performancën e sistemeve dhe adreson çështjet e sigurisë me shpejtësi. • Reagon me shpejtësi ndaj incidenteve dhe shkeljeve të sigurisë. • Kryen analiza për të kuptuar shkallën dhe ndikimin e incidenteve. • Koordinon me ekipet përkatëse për të izoluar dhe zgjidhur kërcënimet. • Dokumenton dhe raporton për incidentet dhe përpjekjet për reagim. • Zhvillon dhe përmirëson planet dhe manualet e reagimit ndaj incidenteve • Mbikëqyr strategjinë dhe zbatimin e mbrojtjes së të dhënave/privacisë. • Ofron trajnime për masat e sigurisë që janë implementuar në institucion.

Ekspert i jashtëm	• Kryen vlerësime të rrezikut dhe teste ndërhyrjeje për të identifikuar dobësitë. • Kryen vlerësime të ndikimit të mbrojtjes së të dhënave / privatësisë. • Monitoron sistemet dhe rrjetin për aktivitete të dyshimta. • Analizon shkeljet e sigurisë dhe dobësitë potenciale.
Departamenti i Auditimit IT	• Ofron trajnime për punonjësit e KLSH-së, për ndërgjegjësimin mbi sigurinë dhe aktet ligjore/nenligjore në këtë drejtim. • Ofron trajnime për principet e mbrojtjes së të dhënave dhe praktikat e mira. • Mbështet strukturën e Auditit të Brendshëm për kryerjen e auditimeve për të siguruar përputhshmërinë me politikat e sigurisë.
Auditi i brendshëm	• Kryen auditime periodike për të siguruar përputhshmërinë me politikat e sigurisë. • Koordinon vlerësimet e sigurisë, auditimet dhe kontrollet e përputhshmërisë.
Të gjithë punonjësit	• Ndjekin dhe zbatojnë udhëzimet e përcaktuara në politikat e sigurisë dhe të raportojnë çështje apo raste të cënimit të sigurisë.

5. Menaxhimi i Rrezikut të Sigurisë së Informacionit

Kontrolli i Lartë i Shtetit do të zhvillojë dhe zbatojë një proces të menaxhimit të rrezikut që përfshin identifikimin, vlerësimin dhe trajtimin e rreziqeve që lidhen me sigurinë e informacionit. Rreziqet do të vlerësohen rregullisht dhe masat e kontrollit do të përmirësohen në përputhje me rezultatet e vlerësimeve.

Kriteret e riskut do të jenë sipas modelit në tabelën e mëposhtme:

Impakti (1-4 nga poshtë lartë)	**Mundësia (1-4 nga e majta në të djathtë)**			
	E Rrallë	E pamundur	E mundur	E pritshme
Shumë i lartë	4	8	12	16
I lartë	3	6	9	12
I mesëm	2	4	6	8
I ulët	1	2	3	4

Vlerësimi dhe veprimet e ndërmarra do të kategorizohen sipas tabelës së mëposhtme:

Vlerësimi (Mundësia x Impakti = Rendësia)		**Veprim**
1-3	Rëndësia e ulët	Nuk kërkohet veprim
4-6	Rëndësia e mesme	Kërkohet monitorim
8-9	Rendësia e lartë	Masa për të lehtësuar
12-16	Rëndësia ekstremisht e lartë	Veprim i menjëhershëm Raportoni te menaxhmenti

6. Menaxhimi i Aseteve

Menaxhimi i aseteve kryhet në përputhje me dispozitat e Ligjit Nr. 10296, datë 08/07/2011, "Për Menaxhimin Financiar dhe Kontrollin", i ndryshuar, në të cilin citohet: "*Të gjitha njësitë e sektorit publik janë të detyruara të ndërmarrin të gjitha masat organizative dhe teknike të nevojshme për administrimin dhe mbrojtjen e aseteve për të siguruar menaxhimin e tyre efektiv dhe për t'i mbrojtur ato nga dëmtimi dhe keqpërdorimi.*"

Inventari i Aseteve: Inventari do të mbahet për të gjitha asetet Hard dhe Soft të teknologjisë së informacionit nga Drejoria e TIK. Për të identifikuar asetet informuese të institucionit dhe për të përcaktuar nivelin e duhur të mbrojtjes, duhet të dokumentohet dhe mbahen një inventar i të gjitha aseteve kritike informuese që zotëron KLSH.
Asetet e informacionit përfshijnë, por nuk kufizohen në:

- Aplikacione/ Sisteme Software;
- Hardware, duke përfshirë pajisjet mobile (laptopët, printerët, etj.);
- Të gjitha asetet e tjera informuese, përfshirë bazat e të dhënave, kontratat dhe marrëveshjet, dokumentacionin e sistemeve të informacionit, manualet e përdoruesit, materialet e trajnimit, procedurat operacionale dhe mbështetëse, planet e vazhdimësisë së **aktiviteteve të institucionit** dhe informacionin e arkivuar.

Pronësia dhe Klasifikimi: Është e rëndësishme të identifikohen se cilat asete kanë nevojë për mbrojtje, kush është përgjegjës për mbrojtjen e tyre, dhe cili është niveli i mbrojtjes që kërkohet.
Asetet e informacionit duhet të trajtohen dhe ruhen për të parandaluar zbulimin e paautorizuar ose keqpërdorimin e informacionit në përputhje me Politikat e Sigurisë së Informacionit.
Klasifikimi i informacionit është thelbësor për sigurinë e informacionit në KLSH. Ky klasifikim përfshin:

- Sigurimin që informacioni ka një nivel të përshtatshëm mbrojtjeje;
- Lejimin që punonjësit të identifikojnë dhe të zbatojnë kërkesat ligjore për trajtimin dhe zbulimin e informacionit thjesht, njëlloj dhe në mënyrë të sigurt.

Të gjitha informacionet, proceset dhe produktet e punës do të klasifikohen, pavarësisht nëse informacioni është publik apo për përdorim të brendshëm.
Çdo kush që përgatit një dokument ose krijon informacion është gjithashtu përgjegjës për klasifikimin e tij në lidhje me kërkesat për konfidencialitet, integritet dhe disponueshmëri.

Përgjegjësitë për asetet: Inventarët e aseteve të informacionit do të dokumentohen, ruhen dhe verifikohen rregullisht, në varësi të rëndësisë dhe vlerës së aseteve.

Të gjitha asetet e informacionit duhet të kenë një punonjës "pronarë" të caktuar. Këta pronarë janë përgjegjës për kontrollin e zhvillimit, mirëmbajtjes, përdorimit dhe sigurisë së aseteve informuese brenda juridiksionit të tyre.
Punonjësit duhet të kthejnë asetet që kanë përdorur pas përfundimit të punës ose ndërrimit të pozita brenda tre ditëve nga përfundimi i marrëdhënies së punës. Nëse këta punonjës nuk mund të jenë të pranishëm për arsye objektive, dorëzimi do të kryhet në praninë e një anëtari të caktuar të komisionit të autorizuar nga thirrja e një anëtari të moshuar të familjes. Nëse punonjësit refuzojnë, dorëzimi do të ndodhë vetëm në praninë e komisionit tw ngritur pwr këtë qëllim.
Kthimi i aseteve në posedim të punonjësve pas përfundimit të punës dokumentohet duke përdorur procedurat standarde. Këto procedura sigurojnë kthimin e:

- Dokumenteve, të dhënave dhe manualeve në çdo format, duke përfshirë asetet informuese të zhvilluara ose përgatitura nga punonjësi ose kontraktori gjatë detyrave të tij;
- Pajisjeve kompjuterike, software-it dhe pajisjeve mobile si laptop-ë, table-të, USB-të, etj.;
- Verifikimin e aseteve të kthyer sipas inventarëve të aseteve;
- Kompensimin për asetet që nuk janë kthyer, në bazë të kritereve që lidhen me amortizimin dhe vlerën e zëvendësimit të asetit të pa kthyer;

Identifikimin e pajisjeve të qasjes që nuk janë kthyer, kartave dhe çelësave që mund të çojnë në qasje të paautorizuar në sistem, në mënyrë që të mbrohet të dhënat dhe sistemet e sigurisë.

Ruajtja e të dhënave - Backup do të kryhet vetëm për Ecxhange (email) dhe Active Directory (AD).

Të gjithë punonjësit e KLSH kanë përgjegjësi personale për sigurinë e informacionit në të gjitha format e saj. Kjo përgjegjësi përfshin, ndër të tjera, njohjen e rregullave që zbatohen për sigurinë e informacionit dhe përgjegjësinë për saktësinë e informacionit.
Në rast dëmtimi të kompjuterit, humbja e informacionit është në rrezik sepse backup-et nuk kryhen automatikisht. Për informacionin e rëndësishëm të ruajtur lokalisht, punonjësi është përgjegjës për kryerjen e backup-eve manuale.

Pajisjet Mobile

Përdorimi i pajisjeve mobile për të ruajtur ose transportuar informacionin rrit rrezikun e kompromet imit të informacionit. Këto pajisje janë zakonisht të vogla dhe mund të humbasin, vidhen ose dëmtohen lehtësisht. Pajisjet mobile përfshijnë, por nuk kufizohen në, USB-të, hard disqet e jashtme, tablet-ët dhe laptop-ët.
Përdorimi i pajisjeve mobile duhet të menaxhohet dhe kontrollohet për të shmangur çdo rrezik të mundshëm. Proceset për autorizimin e përdorimit të këtyre pajisjeve duhet të dokumentohen. Punonjësit që përdorin pajisje mobile duhet të:

* Të jenë të vetëdijshëm për rreziqet dhe përgjegjësitë shtesë që lidhen me përdorimin e këtyre pajisjeve;

* Të jenë të njohur me masat mbrojtëse që mund të përdoren në këto pajisje dhe kur duhet të aplikohen.

7. Kontrolli i aksesit

Kontrolli i Lartë i Shtetit do të sigurojë procedura të qarta për të kontrolluar aksesin në të gjitha sistemet dhe informacionet e saj, duke përfshirë:

- Procedura për dhënien, heqjen dhe rishikimin e të drejtave bazuar në rolin dhe përgjegjësitë e punonjësve;
- Përgjegjësia e përdoruesve për menaxhimin e fjalëkalimeve dhe kredencialeve për aksesimin në sisteme të ndryshme, fjalëkalimi duhet të jetë me 9 (nëntë) karaktere ku përfshihet shkonjë e madhe, numra dhe simbole. Vlefshmëria e passwordit është 180 ditë, nqs password bëhet 3 (tre) here gabim duhet të kontaktohet stafi IT;
- Përdoruesit nuk kanë akses në Command Prompt, Power Shell;
- Punonjësit nuk do të kenë akses në adresën zyrtare të email-it, nga dita e shkëputjes së marrdhënieve të punës.

8. Siguria fizike dhe ambientale

Zona të Sigurta: Zonat që nevojiten të kenë një siguri fizike dhe ambientale janë: dhoma e serverëve dhe rack-et në çdo kat të ndërtesës ku ndodhen zyrat qendrore të institucionit.
Aksesin në Server Room dhe në Rack-et e kateve të institucionit e kanë vetëm punonjësit e IT që kujdesen për mbarëvajtjen e punës dhe cdo ndryshim që është i nevojshëm.

Siguria e Pajisjeve: Hyrja në dhomën e serverave i lejohet vetëm stafit të Drejtorisë të Teknologjisë së Informacionit. Në rast të hyrjes së dikujt tjetër (persona suporti teknik të jashtëm) duhet bërë verifikimi dhe shoqërimi i tyre gjatë qëndrimit në këtë dhomë. Punonjësi i ngarkuar për pastrimin e institucionit është e detyrueshme të shoqërohet nga një punonjës i Drejtorisë së Teknologjisë së Informacionit për pastrimin e dhomës së serverëve.

9. Menaxhimi i komunikimeve dhe operacioneve

Kontrolli i Lartë i Shtetit do të hartojë dhe vendosë në funksion:

- Procedura për menaxhimin dhe mirëmbajtjen e sistemeve të informacionit;
- Procedura për menaxhimin e ndryshimeve në sistemet e informacionit;
- Procedura për kopjimin dhe rikthimin e të dhënave;
- Procedura kontrolli mbi kapacitetet e pajisjeve për të përballuar ngarkesën;

- Procedura për mbrojtjen kundër malware-it.
- Procedura të kontrollit ditor.

10. Siguria në rrjet

Kontrolli i Rrjetit: Kontrolli i Lartë i Shtetit do të marrë masa për mbrojtjen e rrjeteve dhe linjave të komunikimit të institucionit.
Aksesimi në distancë (remote): Nuk lejohet aksesimi në distancë nëpërmjet programeve që mundësojnë këtë si: TeamViewer, AnyDesk, Microsoft Remote Desktop, LogMeIn, Splashtop, etj.

11. Blerja, zhvillimi dhe mirëmbajtja e sistemeve

Kërkesat për sigurinë e sistemeve të informacionit: Siguria e informacionit do të përfshihet në termat teknikë të hartuar për zhvillimin dhe blerjen dhe mirëmbajtjen e sistemeve të informacionit.
Siguria në proceset e zhvillimit dhe mirëmbajtjes: Do të zbatohen masa sigurie gjatë zhvillimit dhe mirëmbajtjes së sistemeve që institucioni disponon.

12. Kontrolli i furnitorëve dhe palëve të treta

Kontrolli i Lartë i Shtetit do të monitorojë dhe kontrollojë palët e treta që kanë akses në informacion ose sisteme kritike. Marrëveshjet përkatëse të nivelit të shërbimit (Service Level Agreement) do të përfshijnë dispozita për sigurinë e informacionit.

13. Menaxhimi i incidentit të sigurisë së informacionit

Incidentet e sigurisë do të raportohen menjëherë dhe do të trajtohen në përputhje me një plan të menaxhimit të incidenteve, i cili përfshin:
- Identifikimin dhe klasifikimin e incidenteve.
- Përgjigjen e shpejtë për të minimizuar dëmet.
- Hetimin dhe dokumentimin e plotë të çdo incidenti.
- Rishikimi dhe përmirësimi i proceseve për të shmangur incidente të ngjashme në të ardhmen.

14. Menaxhimi i vazhdimësisë së institucionit

Kontrolli i Lartë i Shtetit do të zhvillojë dhe zbatojë një plan për vazhdimësinë e aktiviteteve të institucionit, duke siguruar që operacionet kritike mund të vazhdojnë edhe gjatë situatave emergjente. Kjo përfshin:
- Ruajtje të rregullta të të dhënave.
- Testime periodike të planit të vazhdimësisë.

15. Përputhshmëria me ligjet dhe rregulloret

Kontrolli i Lartë i Shtetit do të sigurohet që aktivitetet e tij janë në përputhje me:

- Ligjin nr.154/2014 "Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit":
- Ligjin nr. 9887 datë 10.03.2008 "Për mbrojtjen e të dhënave personale", i ndryshuar;
- Regulloren e Përgjithshme për Mbrojtjen e të Dhënave GDPR - General Data Protection Regulation, në të cilën përcaktohen detyrimet për përpunimin e të dhënave personale.

Termi "përpunim" nënkupton çdo veprim me të dhënat personale, qoftë dhe thjesht të pasurit akses në këto të dhëna, si dhe për veprime të tjera përpunuese që janë: *mbledhja, organizimi, strukturimi, ruajtja, përshtatja apo ndryshimi, rikthimi, këshillimi, përdorimi, përhapja me anë të transmetimit, shpërndarja ose vënia në dispozicion në një mënyrë tjetër, përafrimi apo kombinimi, kufizimi, arkivimi, fshirja ose shkatërrimi.*

16. Trajnimi dhe ndërgjegjësimi për sigurinë

Kontrolli i Lartë i Shtetit do të ofrojë trajnime të rregullta për të gjithë punonjësit në lidhje me sigurinë e informacionit dhe menaxhimin e rreziqeve. Ndërgjegjësimi për sigurinë është thelbësor për të siguruar që të gjithë janë të informuar për kërcënimet aktuale dhe për mënyrat më të mira për t'i parandaluar ato.

17. Auditimi i brendshëm i sigurisë

Auditimet e brendshme do të kryhen në intervale të rregullta për të siguruar që SMSI është duke funksionuar siç duhet dhe është në përputhje me standardin ISO/IEC 27001:2022. Çdo përmirësim i rekomanduar do të regjistrohet dhe do të zbatohet në mënyrë efektive.

18. Përmirësimi i vazhdueshëm

Kontrolli i Lartë i Shtetit do të angazhohet për përmirësimin e vazhdueshëm të Sistemit të Menaxhimit të Sigurisë së Informacionit, duke rishikuar rregullisht politikat dhe procedurat e sigurisë, si dhe duke vlerësuar rreziqet dhe kërkesat e reja të institucionit dhe të teknologjisë.

19. Detyrimi dhe Pasojat

1. Detyrimi për sigurinë në informacion parashikohet që në fazën e fillimit të marrdhënies së punës, ku çdo punonjës njihet me detyrat dhe detyrimet gjatë ushtrimit të funksionit të përcaktuara në aktet e Kontrollit të Lartë të Shtetit për sistemin e informacionit, duke përcaktuar qartë edhe detyrimet për ruajtjen e informacionit dhe konfidencialitetit.
2. Rregullat dhe pasojat për moszbatimin e tyre përcaktohen në Rregulloren e Brendshme mbi Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit

20. Referenca

Rregullore dhe Metodologji për mbarëvajtjen e politikave:

1. Metodologji për identifikimin, vlerësimin dhe prioritarizimin e rreziqeve;
2. Ligjin specifik për Mbrojtjen e të Dhënave Personale;
3. Vendime/Regullore për Mbrojtjen e të Dhënave Personale;
4. Procedura për nivelet e aksesit bazuar në rolin dhe përgjegjësitë e punonjësve;
5. Procedura manuale për backup.