



**KRYEMINISTRIA**

**AGJENCIA KOMBËTARE PËR SIGURINË KOMPJUTERIKE (ALCIRT)**

**UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE  
SHTETËRORE**

*Miratuar me Urdhrin nr.5 datë 12.04.02016 të  
Drejtorit të Agjencisë Kombëtare për Sigurinë  
Kompjuterike (ALCIRT).*

## **Përmbajtje**

1. Hyrje .....	3
2. Qëllimi .....	3
3. Fusha e zbatimit .....	3
4. Informacion i përgjithshëm .....	3
5. Hyrja në fuqi .....	3
• Tabelat e kontrollit të informacionit .....	4
• Fjalori i Kontrolleve të Sigurisë së informacionit .....	20

## 1. Hyrje

**Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT)** bazuar në Vendimin e Këshillit të Ministrave nr. 945, datë 02.11.2012 “Për Miratimin e Rregullores ‘Administrimi i Sistemit të Bazave të të Dhënave Shtetërore’”, neni 21 ‘Përzgjedhja e masave të sigurisë sipas klasave të sigurisë’, pika 2:

*“Masat e sigurisë përzgjidhen në përputhje me klasën e sigurisë dhe sipas udhëzimeve të nxjerra nga Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT).” ka hartuar këtë udhëzim për masat e sigurisë për bazat e të dhënave shtetërore.*

## 2. Qëllimi

Ky udhëzim përcakton sigurinë bazë të informacionit dhe kontrollet e nevojshme për të mbrojtur në mënyrë të njëtrajtshme konfidencialitetin, integritetin dhe disponueshmërinë e informacionit që administrohet në kuadër të bazave të të dhënave shtetërore.

## 3. Fusha e zbatimit

Zbatimi i këtij udhëzimi është i detyrueshëm për të gjitha bazat e të dhënave shtetërore që janë të parashikuara në Ligjin Nr. 10 325, datë 23.9.2010 “Për Bazat e të Dhënave Shtetërore” dhe akteve nënligjore në zbatim të tij.

## 4. Informacioni i përgjithshëm

Në bazë të politikave të sigurisë së informacionit, çdo klasifikim i informacionit duhet të ketë një bashkësi kontrollesh bazë.

Tabelat e kontrollit për sigurinë e informacionit sipas niveleve të ndikimit (i ulët, i mesëm dhe i lartë) dhe parimeve të sigurisë (konfidencialiteti, integriteti dhe disponueshmëria) gjenden në tabelat me poshtë. Tabelat e kontrollit përmbajnë kontrollet bazë që duhet të implementohen për klasifikimin e informacionit. Ka 18 tabela kontrolli.

Një institucion mund të shtojë më shumë kontrolle, por nuk mund të modifikojë ose të fshijë kontrollet origjinale. Përveç 18 tabelave të kontrollit, është edhe një tabelë përmbledhëse për gjithë kontrollet e konfidencialitetit, integritetit dhe disponueshmërisë. Shpjegime të detajuara për kontrollet e tabelave jepen pas 18 tabelave dhe shpjegimet duhet të përdoren të ndërthurura me këto tabela.

Ky udhëzim synohet të përdoret për të përcaktuar kontrollet e sigurisë së informacionit bazuar në klasifikim, jo në metodat specifike për implementimin e kontrollit.

## 5. Hyrja në fuqi

Ky udhëzim do të hyjë në fuqi pas miratimit nga Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT), si dhe do të publikohet në Buletinin e Njoftimeve Publike. Udhëzuesi do të rishikohet të paktën një herë në vit për të siguruar përshtatshmërinë.

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

- Tabelat e kontrollit të informacionit

Menuja e vlerësimit të klasifikimit

Numri #	Vlerësimi i klasifikimit	Klasa e sigurisë	Konfidencialiteti	Integriteti	Disponueshmëria
A-1	UUU	U	K1	I1	D1
A-2	UUM	M	K1	I1	D2
A-3	UUL	L	K1	I1	D3
A-4	UMU	M	K1	I2	D1
A-5	UMM	M	K1	I2	D2
A-6	UML	L	K1	I2	D3
A-7	ULU	L	K1	I3	D1
A-8	ULM	L	K1	I3	D2
A-9	ULL	L	K1	I3	D3
A-10	MUU	M	K2	I1	D1
A-11	MUM	M	K2	I1	D2
A-12	MUL	L	K2	I1	D3
A-13	MMU	M	K2	I2	D1
A-14	MMM	M	K2	I2	D2
A-15	MML	L	K2	I2	D3
A-16	MLU	L	K2	I3	D1
A-17	MLM	L	K2	I3	D2
A-18	MLL	L	K2	I3	D3

A-1

KONFIDENCIALITETI (K): I ULËT		INTEGRITETI (I): I ULËT		DISPONUESHMËRIA (D): I ULËT	
Referenca për në shtojcën B	R = I detyrueshëm	O = Opsional			KID
Kontrollet e Institucioneve Shtetërore					
1	R Procesi i aprovimit/mohimit të aksesit				K
18	R Klasifikimi dhe inventarizimi i informacionit				KID
Kontrollet e zotëruesit të informacionit					
2	R Aksesit i autorizuar nga zotëruesi i informacionit				K
26	R Rishikimi i listave të aksesit				KI
28	R Rishikimi dhe riklasifikimi i informacionit				KID

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

Kontrollet e ruajtësit të informacionit		
9	R Validimi bazë i të dhënave hyrëse	I
15	R Fshirja e pajisjeve të ri-shkrueshme përpara ripërdorimit	K
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “ Konfidencialiteti – I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

A-2

<b>KONFIDENCIALITETI (K): I ULËT</b>	<b>INTEGRITETI (I): I ULËT</b>	<b>DISPONUESHMËRIA (D): MESATARE</b>
Fjalori X-ref #	R = I detyrueshëm    O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
18	R Klasifikimi dhe inventarizimi i informacionit	KID
Kontrollet e zotëruesit të informacionit		
2	R Aksesit i autorizuar nga zotëruesi i informacionit	K
4	R Aksesit i ofruar për më shumë se një person	D
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masa për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “ Konfidencialitet – I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshme	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

A-3

<b>KONFIDENCIALITETI (K): I ULËT</b>		<b>INTEGRITETI (I): I ULËT</b>	<b>DISPONUESHMËRIA (D): E LARTË</b>
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID
<b>Kontrollet e Institucioneve Shtetërore</b>			
1	R Procesi i aprovimit/mohimit të aksesit		K
5	R Hartimi i planit të vazhdimësisë së biznesit/Disaster Recovery Plan		D
18	R Klasifikimi dhe inventarizimi i informacionit		KID
<b>Kontrollet e zotëruesit të informacionit</b>			
2	R Aksesit i autorizuar nga zotëruesi i informacionit		K
4	R Aksesit i ofruar për më shumë se një person		D
26	R Rishikimi i listave të aksesit		KI
28	R Rishikimi dhe riklasifikimi i informacionit		KID
<b>Kontrollet e ruajtësit të informacionit</b>			
6	R Mjete alternative të disponueshmërisë		D
8	R Procedurat e Backup dhe Recovery		ID
9	R Validimi bazë i të dhënave hyrëse		I
13	R Masa për mbrojtjen e mjedisit		ID
14	R Monitorimi i masave për mbrojtjen e mjedisit		ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit		K
23	R Off-site Backup		D
24	R Backup sistematik		ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme		K
<b>Kontrollet e përdoruesit të informacionit</b>			
19	O Emërtimi: “Konfidencialitet – I Ulët”		K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe		K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>			
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë		KID

A-4

<b>KONFIDENCIALITETI (K): I ULËT</b>		<b>INTEGRITETI (I): MESATAR</b>	<b>DISPONUESHMËRIA (D): I ULËT</b>
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID
<b>Kontrollet e Institucioneve Shtetërore</b>			
1	R Procesi i aprovimit/mohimit të aksesit		K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
Kontrollet e zotëruesit të informacionit		
2	R Aksesit i autorizuar nga zotëruesi i informacionit	K
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masa për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të ri-shkrueshme përpara ripërdorimit	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “Konfidencialitet – I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

A-5

<b>KONFIDENCIALITETI (K): I ULËT</b>	<b>INTEGRITETI (I): MESATAR</b>	<b>DISPONUESHMËRIA (D): MESATARE</b>
Fjalori X-ref #	R = I detyrueshëm    O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
Kontrollet e zotëruesit të informacionit		

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËTËRORE

2	R Aksesi i autorizuar nga zotëruesi i informacionit	K
4	R Aksesi i ofruar për më shumë se një person	D
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masa për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të ri-shkrueshme përpara ripërdorimit	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “Konfidencialitet – I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

A-6

KONFIDENCIALITETI (K): I ULËT		INTEGRITETI (I): MESATAR	DISPONUESHMËRIA (D): E LARTË
Fjalori X-ref #	R = I detyrueshëm    O = Opsional		KID
Kontrollet e Institucioneve Shtetërore			
1	R Procesi i aprovimit/mohimit të aksesit		K
5	R Hartimi i planit të vazhdimësisë së biznesit/Disaster Recovery Plan		D
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit		I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit		I
18	R Klasifikimi dhe inventarizimi i informacionit		KID
Kontrollet e zotëruesit të informacionit			
2	R Aksesi i autorizuar nga zotëruesi i informacionit		K
4	R Aksesi i ofruar për më shumë se një person		D
26	R Rishikimi i listave të aksesit		KI
28	R Rishikimi dhe riklasifikimi i informacionit		KID
Kontrollet e ruajtësit të informacionit			
6	R Mjete alternative të disponueshmërisë		D
8	R Procedurat e Backup dhe Recovery		ID
9	R Validimi bazë i të dhënave hyrëse		I



UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

13	R Masa për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
23	R Off-site Backup	D
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “Konfidencialitet - I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë ( çdo vit)	KID

A-7

KONFIDENCIALITETI (K): I ULËT		INTEGRITETI (I): I LARTË	DISPONUESHMËRIA (D): I ULËT
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID
Kontrollet e Institucioneve Shtetërore			
1	R Procesi i aprovimit/mohimit të aksesit		K
7	R Ambienti i ruajtjes i aprovuar		KI
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit		I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit		I
18	R Klasifikimi dhe inventarizimi i informacionit		KID
31	R Rishikimi i logeve të sistemit dhe aplikacionit		KI
Kontrollet e zotëruesit të informacionit			
2	R Akses i autorizuar nga zotëruesi i informacionit		K
27	R Rishikimi i listave të aksesit (çdo vit)		KI
28	R Rishikimi dhe riklasifikimi i informacionit		KID
Kontrollet e ruajtjesit të informacionit			
8	R Procedurat e Backup dhe Recovery		ID
9	R Validimi bazë i të dhënave hyrëse		I
13	R Masa për mbrojtjen e mjedisit		ID
14	R Monitorimi i masave për mbrojtjen e mjedisit		ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit		K
21	R Akses i limituar në zonat e sigurta		KI
22	R Integriteti i mesazheve		I
24	R Backup sistematik		ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme		K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

<b>Kontrollet e përdoruesit të informacionit</b>		
19	O Emërtimi: “Konfidencialitet - I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

**A-8**

KONFIDENCIALITETI (K): I ULËT	INTEGRITETI (I): I LARTË	DISPONUESHMËRIA (D): MESATARE
Fjalori X-ref #	R = I detyrueshëm    O = Opsional	KID
<b>Kontrollet e Institucioneve Shtetërore</b>		
1	R Procesi i aprovimit/mohimit të aksesit	K
7	R Ambienti i ruajtjes i aprovuar	KI
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
31	R Rishikimi i logeve të sistemit dhe aplikacionit	KI
<b>Kontrollet e zotëruesit të informacionit</b>		
2	R Aksesit i autorizuar nga zotëruesi i informacionit	K
4	R Aksesit i ofruar për më shumë se një person	D
27	R Rishikimi i listave të aksesit (çdo vit)	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
<b>Kontrollet e ruajtësit të informacionit</b>		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masa për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
21	R Aksesit i limituar në zonat e sigurta	KI
22	R Integriteti i mesazheve	I
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
<b>Kontrollet e përdoruesit të informacionit</b>		
19	O Emërtimi: “Konfidencialitet - I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

A-9

KONFIDENCIALITETI (K): I ULËT	INTEGRITETI (I): I LARTË	DISPONUESHMËRIA (D): E LARTË
Fjalori X-ref #	R = I detyrueshëm O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
5	R Hartimi i Planit të vazhdimësisë së biznesit / Disaster Recovery Plan	D
7	R Ambienti i ruajtjes i aprovuar	KI
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
31	R Rishikimi i logeve të sistemit dhe aplikacionit	KI
Kontrollet e zotëruesit të informacionit		
2	R Aksesit i autorizuar nga zotëruesi i informacionit	K
4	R Aksesit i ofruar për më shumë se një person	D
27	R Rishikimi i listave të aksesit (çdo vit)	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtjesit të informacionit		
6	R Mjete alternative të disponueshmërisë	D
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masa për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
21	R Aksesit i limituar në zonat e limituara	KI
22	R Integriteti i mesazheve	I
23	R Off-site Backup	D
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
19	O Emërtimi: “Konfidencialitet - I Ulët”	K
33	R Përdorimi i metodave të kontrollit për mediat një-përdorimshe	K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

**A-10**

KONFIDENCIALITETI (K): MESATAR	INTEGRITETI (I): I ULËT	DISPONUESHMËRIA (D): E ULËT
Fjalori X-ref #	R = I detyrueshëm O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
12	R Shkatërro kur nuk është më e nevojshme	K
18	R Klasifikimi dhe inventarizimi i informacionit	KID
Kontrollet e zotëruesit të informacionit		
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)	K
26	R Rishikim i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
9	R Validimi bazë i të dhënave hyrëse	I
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
10	R Sigurimi fizik i pajisjeve	K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “Konfidencialiteti – Mesatar”	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

**A-11**

KONFIDENCIALITETI (K): MESATAR	INTEGRITETI (I): I ULËT	DISPONUESHMËRIA (D): MESATARE
Fjalori X-ref #	R = I detyrueshëm O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
12	R Shkatërro kur nuk është më e nevojshme	K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

18	R Klasifikimi dhe inventarizimi i informacionit	KID
<b>Kontrollet e zotëruesit të informacionit</b>		
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)	K
6	R Aksesit i siguar për më shumë se një person	D
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
<b>Kontrollet e ruajtësit të informacionit</b>		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masat për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
<b>Kontrollet e përdoruesit të informacionit</b>		
10	R Sigurimi fizik i pajisjeve	K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “ Konfidencialiteti – Mesatar”	K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

**A-12**

KONFIDENCIALITETI (K): MESATAR	INTEGRITETI (I): I ULËT	DISPONUESHMËRIA (D): E LARTË
Fjalori X-ref #	R = I detyrueshëm    O = Opsional	KID
<b>Kontrollet e Institucioneve Shtetërore</b>		
1	R Procesi i aprovimit/mohimit të aksesit	K
5	R Hartimi i Planit të vazhdimësisë së biznesit / Disaster Recovery Plan	D
12	R Shkatërro kur nuk është më e nevojshme	K
18	R Klasifikimi dhe inventarizimi i informacionit	KID
<b>Kontrollet e zotëruesit të informacionit</b>		
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)	K
6	R Aksesit i siguar për më shumë se një person	D
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
<b>Kontrollet e ruajtësit të informacionit</b>		
6	R Mjete alternative të disponueshmërisë	D
8	R Procedurat e Backup dhe Recovery	ID

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

9	R Validimi bazë i të dhënave hyrëse	I
13	R Masat për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
23	R Off-site Backup	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
<b>Kontrollet e përdoruesit të informacionit</b>		
10	R Sigurimi fizik i pajisjeve	K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “Konfidencialiteti – Mesatar”	K
25	R Tërheqje kur printohet/fax (në kohë)	K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

**A-13**

KONFIDENCIALITETI (K): MESATAR		INTEGRITETI (I): MESATAR	DISPONUESHMËRIA (D): E ULËT
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID
<b>Kontrollet e Institucioneve Shtetërore</b>			
1	R Procesi i aprovimit/mohimit të aksesit		K
12	R Shkatërro kur nuk është më e nevojshme		K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit		I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit		I
18	R Klasifikimi dhe inventarizimi i informacionit		KID
<b>Kontrollet e zotëruesit të informacionit</b>			
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)		K
26	R Rishikimi i listave të aksesit		KI
28	R Rishikimi dhe riklasifikimi i informacionit		KID
<b>Kontrollet e ruajtësit të informacionit</b>			
8	R Procedurat e Backup dhe Recovery		ID
9	R Validimi bazë i të dhënave hyrëse		I
13	R Masat për mbrojtjen e mjedisit		ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit		K
24	R Backup sistematik		ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme		K

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

Kontrollet e përdoruesit të informacionit		
10	R Sigurimi fizik i pajisjeve	K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “ Konfidencialiteti – Mesatar”	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

A-14

KONFIDENCIALITETI (K): MESATAR	INTEGRITETI (I): MESATAR	DISPONUESHMËRIA (D): MESATARE
Fjalori X-ref #	R = I detyrueshëm O = Opsional	KID
Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
12	R Shkatërro kur nuk është më e nevojshme	K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
Kontrollet e zotëruesit të informacionit		
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)	K
4	R Aksesit i ofruar për më shumë se një person	D
26	R Rishikimi i listave të aksesit	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masat për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
10	R Sigurimi fizik i pajisjeve	K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “ Konfidencialiteti – Mesatar”	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
29	R Rishikimi i procedurave dhe kontrolleve të sigurisë	KID

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

**A-15**

KONFIDENCIALITETI (K): MESATAR		INTEGRITETI (I): MESATAR	DISPONUESHMËRIA (D): E LARTË
Fjalori X-ref #	R = I detyrueshëm    O = Opsional		KID
<b>Kontrollet e Institucioneve Shtetërore</b>			
1	R Procesi i aprovimit/mohimit të aksesit		K
5	R Hartimi i Planit të vazhdimësisë së biznesit / Disaster Recovery Plan		D
12	R Shkatërro kur nuk është më e nevojshme		K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit		I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit		I
18	R Klasifikimi dhe inventarizimi i informacionit		KID
<b>Kontrollet e zotëruesit të informacionit</b>			
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)		K
4	R Aksesit i ofruar për më shumë se një person		D
26	R Rishikimi i listave të aksesit		KI
28	R Rishikimi dhe riklasifikimi i informacionit		KID
<b>Kontrollet e ruajtësit të informacionit</b>			
6	R Mjete alternative të disponueshmërisë		D
8	R Procedurat e Backup dhe Recovery		ID
9	R Validimi bazë i të dhënave hyrëse		I
13	R Masat për mbrojtjen e mjedisit		ID
14	R Monitorimi i masave për mbrojtjen e mjedisit		ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit		K
23	R Off-site Backup		D
24	R Backup sistematik		ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme		K
<b>Kontrollet e përdoruesit të informacionit</b>			
10	R Sigurimi fizik i pajisjeve		K
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit		K
20	O Emërtimi: “Konfidencialiteti – Mesatar”		K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>			
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)		KID

**A-16**



UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

KONFIDENCIALITETI (K): MESATAR		INTEGRITETI (I): I LARTË	DISPONUESHMËRIA (D): E ULËT
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID
<b>Kontrollet e Institucioneve Shtetërore</b>			
1	R	Procesi i aprovimit/mohimit të aksesit	K
7	R	Ambjenti i ruajtjes i aprovuar	KI
12	R	Shkatërro kur nuk është më e nevojshme	K
16	R	Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R	Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R	Klasifikimi dhe inventarizimi i informacionit	KID
31	R	Rishikim i logeve të sigurisë të sistemit dhe aplikacioneve	KI
<b>Kontrollet e zotëruesit të informacionit</b>			
3	R	Akresi i autorizuar nga zotëruesi i informacionit (i shkruar)	K
27	R	Rishikimi i listave të aksesit (çdo vit)	KI
28	R	Rishikimi dhe riklasifikimi i informacionit	KID
<b>Kontrollet e ruajtjesit të informacionit</b>			
8	R	Procedurat e Backup dhe Recovery	ID
9	R	Validimi bazë i të dhënave hyrëse	I
13	R	Masat për mbrojtjen e mjedisit	ID
14	R	Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R	Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
21	R	Akses i limituar në zonat e sigurta	K
22	R	Integriteti i mesazheve	I
24	R	Backup sistematik	ID
32	R	Rikuperim testim i të dhënave backup	ID
55	R	Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
<b>Kontrollet e përdoruesit të informacionit</b>			
15	R	Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
32	O	Emërtimi: “Konfidencialiteti – Mesatar”	K
<b>Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)</b>			
30	R	Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

A-17

KONFIDENCIALITETI (K): MESATAR		INTEGRITETI (I): I LARTË	DISPONUESHMËRIA (D): MESATARE
Fjalori X-ref #	R = I detyrueshëm O = Opsional		KID

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

Kontrollet e Institucioneve Shtetërore		
1	R Procesi i aprovimit/mohimit të aksesit	K
7	R Ambienti i ruajtjes i aprovuar	KI
12	R Shkatërro kur nuk është më e nevojshme	K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
31	R Rishikim i logeve të sigurisë të sistemit dhe aplikacioneve	KI
Kontrollet e zotëruesit të informacionit		
3	R Aksesit i autorizuar nga zotëruesi i informacionit (i shkruar)	K
4	R Aksesit i ofruar për më shumë se një person	D
27	R Rishikimi i listave të aksesit (çdo vit)	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtjesit të informacionit		
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masat për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
21	R Akses i limituar në zonat e sigurta	K
22	R Integriteti i mesazheve	I
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	K
20	O Emërtimi: “Konfidencialiteti – Mesatar”	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

A-18

KONFIDENCIALITETI (K): MESATAR		INTEGRITETI (I): I LARTË		DISPONUESHMËRIA (D): E LARTË	
Fjalori X-ref #	R = I detyrueshëm	O = Opsional			KID
Kontrollet e Institucioneve Shtetërore					
1	R Procesi i aprovimit/mohimit të aksesit				K
5	R Hartimi i Planit të vazhdimësisë së biznesit / Disaster Recovery Plan				D
7	R Ambienti i ruajtjes i aprovuar				KI

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHTETËRORE

12	R Shkatërro kur nuk është më e nevojshme	K
16	R Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	I
17	R Plane testimi formale dhe rezultate të dokumentuara për sistemet e informacionit	I
18	R Klasifikimi dhe inventarizimi i informacionit	KID
31	R Rishikim i logeve të sigurisë të sistemit dhe aplikacioneve	KI
Kontrollet e zotëruesit të informacionit		
3	R Akses i autorizuar nga zotëruesi i informacionit (i shkruar)	K
4	R Akses i ofruar për më shumë se një person	D
27	R Rishikimi i listave të aksesit (çdo vit)	KI
28	R Rishikimi dhe riklasifikimi i informacionit	KID
Kontrollet e ruajtësit të informacionit		
6	R Mjete alternative të disponueshmërisë	D
8	R Procedurat e Backup dhe Recovery	ID
9	R Validimi bazë i të dhënave hyrëse	I
13	R Masat për mbrojtjen e mjedisit	ID
14	R Monitorimi i masave për mbrojtjen e mjedisit	ID
15	R Fshirja e pajisjeve të rishkrueshme përpara ripërdorimit	K
21	R Akses i limituar në zonat e sigurta	K
22	R Integriteti i mesazheve	I
23	R Off-site Backup	D
24	R Backup sistematik	ID
34	R Përdorimi i metodave të kontrollit për mediat e rishkrueshme	K
Kontrollet e përdoruesit të informacionit		
11	R Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuarit	K
20	O Emërtimi: “Konfidencialiteti – Mesatar”	K
Kontrollet e Oficerit të Sigurisë së Informacionit (CIO)		
30	R Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	KID

- **Fjalori i Kontrollleve të Sigurisë së informacionit**

**Kontrollet e Impaktit: I ULËT (U), MESATAR (M) dhe I LARTË (L)**

Nr.	Kontrolli	Nevoja	Tipi i kontrollit	Shpjegimi/Qartësimi	KID	Shkalla e kontrollit	Roli i sugjeruar
1	Procesi i aprovimit/mohimit të aksesit	R	Autorizim	Institucionet publike duhet të kenë një proces formal të dokumentuar për të dhënë akses në asetet e tyre të informacionit. Informacioni jepet bazuar në role ose në nevojën për t'u njohur me të. Aksesit jepet për nevoja specifike dhe nuk jepet kur nevoja nuk është më prezente.	K	I ulët	Institucionet publike
2	Aksesi i autorizuar nga zotëruesi i informacionit	R	Autorizim	Përgjegjësinë për autorizimin e aksesit e ka vetëm zotëruesi i informacionit. Përdoruesit që kërkojnë akses duhet të ndjekin procesin e aprovimit të aksesit të institucionit përkatës.	K	I ulët	Zotëruesi i informacionit
3	Aksesi i autorizuar nga zotëruesi i informacionit (i shkruar)	R	Autorizim	Zotëruesi i informacionit duhet të sigurojë autorizim të shkruar për akses. Kjo nuk përfshin proceset rutinë të ditës si për shembull: IT të ketë akses në skedarët për qëllime backup etj. Ky autorizim mund të përfshijë një aprovim për një përdorues ose një grup përdoruesish.	K	Mesatar	Zotëruesi i informacionit
4	Aksesi i ofruar për më shumë se një person	R	Autorizim	Siguron që më shumë se një person ka akses në informacion për qëllime të vazhdimësisë së proceseve të punës.	D	Mesatar	Zotëruesi i informacionit
5	Hartimi i planit të vazhdimësisë së biznesit/Disaster Recovery Plan	R	Backup	Ndërmerret një analizë për të identifikuar proceset kryesore të punës dhe informacionin nga i cili varen. Plan i Vazhdimësisë duhet të përfshijë një	D	I lartë	Institucionet publike

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËTËRORE

				strategji për rikuperimin nga katastrofat me synim që të rifillojë operacionet normale në një afat kohor të arsyeshëm. Procedurat për rikuperimin nga katastrofat duhet të jenë të përditësuara dhe të testohen periodikisht.			
6	Mjete alternative të disponueshmërisë	R	Backup	Duhet të ketë procese të përshtatshme për disponueshmërinë e të dhënave (psh. Hardware <i>redundant</i> , mirroring/replikim/shadowing, site alternative)	D	I lartë	Ruajtësi i informacionit
7	Ambienti i ruajtjes i aprovuar	R	Ruajtje	Ambientet e ruajtjes të aprovuara janë Data Center. Institucionet publike fizikisht sigurojnë serverat qendrorë/ qendrat e të dhënave, dhe facilitete të tjera të aprovuara me shkrim nga drejtuesi i Institucionit shtetëror. Rrjetet e brendshme të komunikimit të të dhënave përfshihen në këtë aprovim.	KI	Mesatar	Institucionet publike
8	Procedurat e Backup-it	R	Backup	Duhet të përcaktohen dhe testohen procedurat e shkruara për rikuperimin e informacionit nga backup-i.	ID	Mesatar	Ruajtësi i informacionit
9	Validimi bazë i të dhënave të inputit	R	Sistemi	Inkorporon kontrollin logjik për informacionin elektronik (psh. Rutina për kontrollin e datës së vlefshme, numri i telefonit nuk duhet të ketë shkronjë, validimi i gjatësive të fushave përpara se të pranojnë të dhëna)	I	I ulët	Ruajtësi i informacionit
10	Sigurimi fizik i pajisjeve	R	Ruajtje	Siguroni fizikisht shkresat dhe/ose pajisjet e ruajtjes elektronike të lëvizshme kur mjedisi i punës është i lirë për të shmangur keqpërdorimin e paqëllimshëm.	K	Mesatar	Përdoruesi

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHTETËRORE

11	Konfirmimi i identitetit dhe të drejtave të aksesit të kërkuesit	R	Shpërndarje	Përpara shpërndarjes së informacionit, verifiko me zotëruesin e informacionit që kërkuesi ka të drejta aksesit legjitime. Verifiko identitetin nëpërmjet njohjes fizike ose fotos së ID.	K	Mesatar	Përdoruesi
12	Shkatërro kur nuk është më e nevojshme	R	Hedhje	Subjekt i kërkesave të sigurisë së institucioneve publike janë: Shkresat – Grisja ose djegia Pajisjet e ruajtjes elektronike – shkatërro duke përdorur metodën më të përshtatshme të caktuar nga Institucionet publike (proceset e fshirjes të cilat duhet të kenë verifikim, grisje) Jeni të vetëdijshëm që disa pajisje (fotokopje, printera, makina fax) kanë hard drives (dmth Imazhi mbet në drive). Është e nevojshme të mbishkruhet duke kopjuar/dërguar faqe bosh. Gjithashtu informacioni mund të qëndrojë në server nëse është printer i rrjetit, në PC locale nëse është printer lokal.	K	Mesatar	Institucionet publike
13	Masat për mbrojtjen e mjedisit	R	Ruajtje	Të ketë pajisje për shuarjen e zjarrit, mbrojtje, energji të pandërprerë (UPS), masa për mbrojtjen ndaj ujit.	ID	Mesatar	Ruajtësi i informacionit
14	Monitorimi i masave për mbrojtjen e mjedisit	R	Ruajtje	Monitoro masat e mbrojtjes së mjedisit dhe përditësoji kur është e nevojshme.	ID	I lartë	Ruajtësi i informacionit
15	Fshirja e mediave të rishkrueshme përpara se të ripërdoren	R	Shpërndarje	Përdor një metodë të fshirjes, të aprovuar nga Institucionet publike. Arsyeja për këtë është se është shumë e vështirë të dish me siguri çfarë klase informacioni ekziston aktualisht ose ka ekzistuar më përpara në media. Është e mundshme që të dhënat të jenë fshirë, por janë ende të rikuperueshme	K	I ulët	Ruajtësi i informacionit

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETETËRORE

				nëpërmjet mjeteve të ndryshme. Mediat përfshijnë hard drives, USB, kartat e memorjes, CD etj.			
16	Procedura formale për ndryshimin e kontrollit për sistemet e informacionit	R	Administrativ	Procedura formale për ndryshimin e kontrollit duhet të ndiqen kur ndodh ndryshim konfigurimi (në aplikacion, softuer, harduer). Për ndryshime emergjente, duhet të ketë masa për rishikim dhe vlerësim të mëtejshëm. Nëse është e nevojshme, ndryshimet duhet të rimerren duke ndjekur procedurën normale për ndryshimin e kontrollit dhe të hiqen ndryshimet emergjente.	I	Mesatar	Institucionet publike
17	Plane testimi formale dhe rezultate të dokumentuarapër sistemet e informacionit	R	Adminstrativ	Planet për testimin e aplikimeve dhe programeve duhet të përcaktohen dhe dokumentohen. Kjo përfshin: metodën e testimit, kriteret për përmbushjen e testit, kriteret për përfundimin e testit dhe pranueshmërinë e përdoruesit. Duhet mbajtur përmbledhje të përfundimeve nga këto teste.	I	Mesatar	Institucionet publike
18	Klasifikimi dhe inventarizimi i informacionit	R	Administrativ	1. Klasifiko asetet e informacionin në mënyrë të vazhdueshme. Klasifikimi i informacionit duhet të jetë i disponueshëm për të gjithë përdoruesit. 2. Mbaj një inventar të shkruar ose elektronik të gjithë asetëve të informacionit.	KID	I ulët	Institucionet publike
19	Emërtimi “Konfidencialiteti – I Ulët”	O	Etiketimi	Nëse zgjidhet për të etiketuar shkresat ose mediat elektronike të portueshme, përdoret etiketa “Konfidencialiteti – I Ulët”. Kjo nuk zëvendëson strukturat e brendshme të	K	I ulët	Përdoruesi

UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETETËRORE

				etiketimit, por duhet të përfshihet kur etiketimi përdoret për të lehtësuar aplikimin uniform të kontrolleve kur informacionin ndahet midis institucioneve.			
20	Emërtimi “Konfidencialiteti – Mesatar”	O	Etiketimi	Nëse zgjidhet për të etiketuar shkresën ose mediat elektronike të portueshme, përdoret etiketa “Konfidencialiteti Mesatar”. Kjo nuk zëvendëson strukturat e brendshme të etiketimit, por duhet të përfshihet kur etiketimi përdoret për të lehtësuar aplikimin uniform të kontrolleve kur informacionin ndahet midis institucioneve.	K	mesatar	Përdoruesi
21	Akses i limituar në zonat e sigurta	R	Autorizim	Aksesi jepet në zonat e sigurta për një nevojë specifike dhe hiqet nëse nevoja nuk është më prezente.	KI	I lartë	Ruajtësi i informacionit
22	Integriteti i mesazheve	R	Autentikim	Për të dhënat elektronike në lëvizje në rrjetat e ndryshme (Internet, GovNet), teknikat e kontrollit të integritetit si kodet e autentikimit të mesazheve, firmat dixhitale ose hashet kriptografike duhet të implementohen në nivel aplikimi. Metodat për çertifikimin e integritetit të të dhënave dhe të dërguesit duhet të përdoren kur dërgohen të dhëna në rrjet me mbrojtje të pamjaftueshme.	I	I lartë	Ruajtësi i informacionit
23	Off-site backup	R	Ruajtje	Kopjet e backup të pajisjeve elektronike të ruajtjes duhet të vendosen në një site të sigurtë sekondar të përshtatshëm të aprovuar nga Institucionet publike.	D	I lartë	Ruajtësi i informacionit
24	Backup sistematik	R	Backup	Zotësuesi i informacionit përcakton kërkesat e backup-it për mediat elektronike në konsultim me ruajtësin. Ruajtësi i	ID	Mesatar	Ruajtësi i informacionit



UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETËRORE

				informacionit i bën backup të dhënave në përputhje me këto kërkesa.			
25	Tërheqje kur printohet/fax (në kohë)	R	Riprodhim	Ndërsa printohet, fotokopjohet, ose dërgohet fax mos lejoni përgjimin dhe të jeni të vetëdijshëm për personat rreth jush. Tërhiqe informacionin menjëherë.	K	Mesatar	Përdoruesi
26	Rishikimi i listave të aksesit	R	Autorizim	Zotëruesi i informacionit rishikon dhe aprovon listat e kontrollit të aksesit (dmth. kush ka akses) në një interval të dokumentuar të përcaktuar nga Institucionet publike.	KI	I ulët	Pronari
27	Rishikimi i listave të aksesit (çdo vit)	R	Autorizim	Zotëruesi i informacionit rishikon dhe aprovon listat e kontrollit të aksesit (dmth. kush ka akses) minimalisht çdo vit.	KI	Mesatar	Pronari
28	Rishikimi dhe riklasifikimi i informacionit	R	Administrativ	Pronarët e informacionit janë përgjegjës për rishikimin dhe riklasifikimin (nëse është e nevojshme) të informacionit që ata zotërojnë në një interval të dokumentuar të caktuar nga Institucionet publike.	KID	I ulët	Pronari
29	Rishikimi i procedurave dhe kontrolleve të sigurisë	R	Administrativ	Rishiko përshtatshmërinë e procedurave dhe kontrolleve të sigurisë në një interval të dokumentuar të caktuar nga Institucionet publike.	KID	I ulët	CIO
30	Rishikimi i procedurave dhe kontrolleve të sigurisë (çdo vit)	R	Administrativ	Rishiko përshtatshmërinë e procedurave dhe kontrolleve të sigurisë minimalisht çdo vit.	KID	I lartë	CIO
31	Rishikim i logeve të sigurisë së sistemit dhe aplikacionit	R	Autorizim	Log-et e sigurisë duhet të analizohen në kohë reale.	KI	I lartë	Institucionet publike
32	Rikuperim testim i të dhënave të backup-it	R	Backup	Verifiko që të dhënat e backup-it elektronik të jenë të rikuperueshme në një bazë dy-vjetore. Objektivat e rikuperimit përcaktohen dhe dokumentohen.	IA	I lartë	Kujdestari (roja)

## UDHËZIM PËR MASAT E SIGURISË PËR BAZAT E TË DHËNAVE SHETETËRORE

33	Përdorimi i metodave në dispozicion për shkresat apo mediat një përdorimshe	R	Dispozicioni	Përdorimi i metodave në dispozicion për hedhjen në kosh apo riciklim	K	I ulët	Përdoruesi
34	Përdorimi i metodave në dispozicion për median e rishkrueshme	R	Dispozicioni	<p>Për pajisjet ruajtëse elektronike (që janë funksionale apo jo) shkatërrimi bëhet me metodën më të përshtatshme të aprovuar nga Institucioni Shtetëror. Arsyeja është sepse është shumë e vështirë për të ditur me siguri cilat klasa të sigurisë së informacionit ekzistojnë apo ekzistojnë në ato pajisje. Nëse të dhënat e pajisjes janë fshirë, ekziston mundësia që të rikthehen me programe të caktuara. Pajisjet përfshijnë usb, hard disqe, karta ose çipe memorie, CD etj.</p> <p>Disa pajisje si printerat, fotokopjet, makinat e faksit etj, kanë hard driver (psh. imazhet qëndrojnë në pajisje). Mund të nevojitet që të rishkruhet memoria me faqe bosh (të bardha) për të pasur mundësinë e rishkrimit. Gjithashtu, informacioni mund të mbetet në serverin e printerit të rrjetit ose në kompjuterin personal nëse printer është lokal.</p>			