Referenca	Tipologjia	Nr. Prot/Data	Klasifikimi	Zotëruesi	Version	Data	Faqe
ISO-SC-023	**Politikë**	.....	**Publik**	**ITS**	**02**	**23.06.2025**	**1/85**

Titulli i dokumentit

Politika e Sigurisë e Sistemeve të Informacionit

REPUBLIKA E SHQIPËRISË

Shoqëria Aksionare për Prodhimin dhe Shpërndarjen e Dokumenteve Biometrike

identiTek

Politika e Sigurisë e Sistemeve të Informacionit

Pronë e IdentiTek Ndalohet Riprodhimi në Çfarëdo Formë

PËRMBAJTJA

1. HYRJE

Kjo është Politika e Sigurisë së Sistemit të Informacionit e IdentiTek.

Ky dokument është një dokument në përditësim të vazhdueshëm. Siguria është një proces në zhvillim të vazhdueshëm, ku pika e fundit kurrë nuk arrihet asnjëherë plotësisht, por i përafrohemi me përpjekje të përditshme dhe duke ecur gjithmonë në drejtimin e duhur. Qasja e ndjekur këtu është të krijohet një set i përcaktuar i politikave dhe procedurave të projektuara për të zvogëluar impaktin e vulnerabiliteteve, kërcënimeve, sulmeve, humbjes apo cenimit të të dhënave.

Ky dokument është projektuar për të ofruar sigurinë e përgjithshme të të gjithë të dhënave, sistemeve, rrjeteve dhe operacioneve të IDENTITEK. Përqasja për sigurinë është e tillë që të mbrojë të dhënat personale të qytetarëve Shqiptarë si edhe burimet e të dhënave në Institucion, por jo të komplikojë ose të ngadalësojë aksesin në informacionin që përdoruesit, operatorët, klientët apo administratorët kanë të nevojshme për të kryer punën e tyre të përditshme. Qëllimi është që ky dokument të jetë në përditësim të vazhdueshëm, për të përfshirë në të, teknologji dhe praktika të reja për forcimin e mëtejshëm të Sigurisë të Institucionit IDENTITEK.

Ky dokument do të përdoret si bazë si për stafin menaxhues ashtu edhe për stafin e Divizionit të Sistemeve të Informacionit për të vlerësuar masat dhe praktikat e duhura të sigurisë ashtu edhe për të projektuar një sistem që siguron një nivel të kënaqshëm sigurie dhe efikasiteti në punë për stafin që operon brenda Perimetrit të ISMS IdentiTek dhe drejtuesit e Institucionit.

Ky dokument trajton të gjitha aspektet e sigurisë së informacionit - sigurinë e rrjetit, perimetrin e jashtëm, ashtu edhe sigurinë e të dhënave në zyrat qendrore apo dhe në stacionet e regjistrimit/shpërndarjes të operuara nga punonjësit e Institucionit.

Përqasja për Sigurinë e të dhënave është jo vetëm nga pikëpamja e ndërhyrjeve keqdashëse, por gjithashtu edhe nga pikëpamja e integritetit të brendshëm, ku gjithashtu konsiderohen si kërcënime: humbja e të dhënave për shkak të korruptimit, fshirjes aksidentale, rrjedhja e informacionit jashtë Institucionit, shkatërrimit të të dhënave nga programe kompjuterike si “virus, “ransomware”, madje edhe të ndonjë modifikim i paautorizuar, abuzimi me postën elektronike apo përfaqësimi i gabuar i Institucionit që mund të kërcënojnë reputacionin e Institucionit.

Pikat kryesore të këtij dokumenti janë përfshirë në 'Politikën e Sigurisë dhe Përdorimit të Pranueshëm' të IDENTITEK, e cila përcakton informacionin e përshtatshëm që përdoruesit, operatorët, administratorët, apo furnizuesit të përdorin informacionet apo resurset në siguri të plotë. Përpara se t'u jepet akses në rrjetet e IDENTITEK, secili përdorues, operator, administrator, furnizues apo

nënkontraktor, nënshkruan një marrëveshje, ku deklaron se ata kuptojnë dhe kanë ndërmend të respektojnë plotësisht këto politika.

Kjo rregullore është në përputhje me Ligjin Nr. 25/2024 "*Për Sigurinë Kibernetike*" dhe përmbush të gjitha kërkesat e përcaktuara në Nenin 20 "Masat e Sigurisë Kibernetike" për masat organizative që një infrastrukture kritike duhet të zbatojë. Kjo rregullore gjithashtu përputhet me standardin ISO 27001, i cili është arkivi i praktikave më të mira të sigurisë.

1.1. Çfarë është Siguria e Informacionit

Informacioni është aset kritik për Institucionin, prandaj është shumë e rëndësishme që të njihet rëndësia që ka mbrojtja e informacionit përmes vendosjes dhe menaxhimit të kontrolleve dhe mekanizmave të përshtatshme dhe efektivë të sigurisë, për t'u mbrojtur nga qasja apo përdorimi i paautorizuar.

Siguria e informacionit përcaktohet si mbrojtja e elementeve të mëposhtme:

- **Konfidencialiteti** - garanton që informacioni është i aksesueshëm vetëm nga persona të autorizuar.
- **Integriteti** – garanton mbrojtjen e plotësisë, saktësisë dhe siguron që nuk ka ndërhyrje apo ndryshime të paautorizuara të informacionit.
- **Disponueshmëria** - garanton që përdoruesit e autorizuar kanë qasje në informacion sa herë që është e nevojshme.

Siguria e informacionit arrihet përmes zbatimin të kontrolleve dhe mekanizmave të përshtatshëm të sigurisë (politika, praktika, procedura, strukturat e menaxhimit të sigurisë dhe produktet e sigurisë).

Këto kontrolle dhe mekanizma vendosen për të siguruar arritjen e qëllimeve të biznesit dhe sigurisë së Institucionit.

1.2. Përse nevojitet Siguria e Informacionit

Shoqëria aksionare IdentiTek me kapital tërësisht shtetëror e krijuar me VKM Nr. 80, datë 14.02.2023, "Mbi krijimin e shoqërisë aksionare për prodhimin dhe shpërndarjen e dokumenteve biometrike", prodhon dhe shpërndan Letërnjoftimet Elektronike, Lejet e Qëndrimit dhe Pasaportat Biometrike. Informacioni i identitetit të qytetarëve duhet të grumbullohet për të mundësuar prodhimin dhe dorëzimin e Letërnjoftimeve Elektronike, Lejeve të Qëndrimit dhe Pasaportave Biometrike.

Shoqëria IdentiTek SHA është krijuar për të garantuar furnizimin e qytetarëve Shqiptarë me dokumente identiteti dhe gjithashtu shërbime elektronike të besuara, bazuar në certifikatat elektronike të qytetarëve, të vendosura në Letërnjoftimet Elektronike dhe Lejet e Qëndrimit.

IdentiTek duhet të jetë në përputhje të plote me Ligjin dhe rregulloret Shqiptare mbi mbrojtjen e të dhënave të qytetarëve dhe gjithashtu duhet të jetë në përputhje me rregulloret e Ofruesve të Kualifikuar të Shërbimeve të Besuara.
Kërcënimet ndaj sigurisë mund të vijnë nga një shumëllojshmëri burimesh të ndryshme, përfshirë këtu mashtrimin e ndihmuar nga kompjuteri, spiunazhin industrial, sabotazhin, vandalizmin apo dhe katastrofë natyrore. Viruset kompjuterikë, hakerimi i paligjshëm dhe sulmet me refuzim të shërbimit janë shembuj të ndryshëm të kërcënimeve të ndeshura gjatë operimit në internet. Këto lloje të kërcënimeve po bëhen gjithnjë e më të zakonshme, më ambicioze dhe më të sofistikuara.

1.3. Si vendosen Kërkesat e Sigurisë

Ky seksion përcakton se si IdentiTek vendos kërkesat e sigurisë.

Ka tre burime kryesore:

- Burimi i parë del nga vlerësimi i rreziqeve për organizatën. Nëpërmjet vlerësimit të rreziqeve, identifikohen kërcënimet ndaj aseteve, vlerësohet vulnerabiliteti dhe mundësia që të ndodhë një ngjarje, dhe kështu vlerësohet ndikimi potencial.
- Burimi i dytë janë kërkesat ligjore, statutore, rregullatore dhe kontraktuale që duhet të plotësojë një organizatë, partnerët e saj tregtarë, kontraktorët si edhe ofruesit e shërbimeve.
- Burimi i tretë është grupi i veçantë i parimeve, objektivave dhe kërkesave për procesimin e informacionit, që një organizatë zhvillon për të mbështetur operacionet e saj.

Ky seksion shpjegon komponentët kritikë të menaxhimit të sigurisë dhe shpreh politikën e IdentiTek në lidhje me analizën e riskut, menaxhimin e riskut, ndështkimin dhe politikën e sigurisë në përgjithësi.

Këto politika dhe standarde përcaktojnë rregullat dhe kërkesat e tjera të nevojshme për operimin e sigurt dhe të besueshëm të infrastrukturës së sistemeve të informacionit të Shoqërisë.

Ka role dhe detyra përkatëse për sigurinë e informacionit për çdo punonjës, kontraktor dhe konsulent në Shoqëri. Është përgjegjësia dhe detyra e punonjësve, kontraktorëve dhe konsulentëve që të raportojnë problemet e sigurisë së informacionit. Institucioni është i detyruar të përfshijë masat e nevojshme të sigurisë, siç është qasja e kufizuar e përdoruesve bazuar në parimin "Nevoja për të ditur".

Këto politika dhe standarde gjithashtu përcaktojnë masat "bazë" të kontrollit, të cilat pritet që të gjithë në Institucion t'i njohin dhe t'i ndjekin në mënyrë konsistente. Në disa raste quhen masat "standard të kujdesit të duhur", këto masa sigurie janë minimumi i kërkuar për të parandaluar një shumëllojshmëri të problemeve të ndryshme, duke përfshirë mashtrimin dhe keqpërdorimin, spiunazhin industrial, sabotazhin, gabimet dhe neglizhencën, si dhe paditë ligjore apo mos disponueshmërinë e sistemit. Në një nivel tjetër, këto politika përcaktojnë gjithashtu kontrollet minimale të nevojshme për të parandaluar probleme ligjore, siç janë akuzat e pakujdesisë, shkelja e detyrave të besnikërisë ose shkelja e privatësisë. Këto politika dhe standarde, detajojnë mënyra të arsyeshme dhe praktike për të gjithë personat në Institucion për të parandaluar humbjet e panevojshme dhe për të mbrojtur të dhënat private të qytetarëve Shqiptarë.

1.4. Vlerësimi i Rreziqeve të Sigurisë

Kërkesat e sigurisë përcaktohen nga një vlerësim metodik të rreziqeve të sigurisë. Për të vlerësuar rreziqet e Institucionit përdoret metodologjia EBIOS dhe gjithashtu huazohet edhe metodologjia ISO 27005.

Shpenzimet për kontrollet duhet të balancohen përkundrejt dëmtimit të biznesit që me gjasa ndodh si rezultat i dështimeve në Siguri. Teknikat e vlerësimit të rreziqeve aplikohen në të gjithë organizatën, ose vetëm në disa pjesë të saj, si edhe në sisteme individuale të informacionit, pjesë specifike të sistemit ose në shërbime ku është e aplikueshme, praktike, dhe realisht ndihmëse.

Vlerësimi i rrezikut është një vlerësim sistematik i:

- Dëmit të mundshëm ndaj biznesit që mund të rezultojë nga një dështim i sigurisë, duke marrë parasysh pasojat potenciale të humbjes së konfidencialitetit, integritetit ose disponueshmërisë së informacionit dhe të aseteve të tjera;
- Mundësisë realiste që një dështim i tillë të ndodhë, në kuadër të kërcënimeve dhe të dobësive aktuale, dhe kontrolleve përkatëse të implementuara aktualisht.

Rezultatet e këtij vlerësimi do të ndihmojnë në udhëzimin dhe përcaktimin e veprimeve dhe prioriteteve të përshtatshme për menaxhimin e rreziqeve të sigurisë së informacionit, dhe për implementimin e kontrolleve të zgjedhura për të mbrojtur kundër këtyre rreziqeve. Procesi i vlerësimit të rreziqeve dhe zgjedhjes së kontrolleve mund të duhet të kryhet disa herë për të mbuluar pjesë të ndryshme të organizatës ose sistemeve të veçanta të informacionit.

Është e rëndësishme të kryhen rishikime periodike të rreziqeve të sigurisë dhe kontrolleve të implementuara për:

- të marrë në konsideratë ndryshimet në kërkesat dhe prioritetet e Institucionit;
- të konsideruar kërcënimet dhe dobësitë e reja;
- të konfirmuar se kontrollet mbeten efektive dhe të përshtatshme;
- të marrë në konsideratë ndryshimet legjislative të Republikës së Shqipërisë.

Rishikimet kryhen në nivele të ndryshme thellësie, në varësi të rezultateve të vlerësimeve të mëparshme dhe niveleve të ndryshme të rrezikut që drejtuesit e Institucionit janë të gatshëm të pranojnë. Vlerësimet e rreziqeve shpesh kryhen fillimisht në një nivel të lartë, si një mjet për të prioritizuar burimet në zonat me rrezik të lartë, dhe më pas në një nivel më të detajuar, për të adresuar rreziqe specifike.

1.5. Përzgjedhja e Kontrolleve

Pas identifikimit të kërkesave për sigurinë e informacionit, IdentiTek vlerëson dhe zgjedh për të zbatuar kontrollet dhe mekanizmat e përshtatshëm të sigurisë, në mënyrë që rreziqet të zvogëlohen në një nivel të përshtatshëm (siç është përcaktuar nga drejtuesit ekzekutiv).

Kontrollet dhe mekanizmat e përshtatshëm të sigurisë vlerësohen dhe zgjidhen bazuar në kosto të lidhura me implementimin e tyre, lidhur me rreziqet që po zvogëlohen dhe humbjet potenciale që mund të rezultojnë nëse ndodh një shkelje e sigurisë. Humbja potenciale e besimit dhe besueshmërisë së klientëve (reputacioni i shoqërisë) merret në konsideratë gjatë përzgjedhjes së kontrolleve dhe mekanizmave të përshtatshëm të sigurisë.

1.6. Pika Fillestare e Sigurisë së Informacionit

Ky dokument ofron detajet e politikave dhe procedurave të përgjithshme të sigurisë për IdentiTek dhe është një dokument në zhvillim që përditësohet dhe referohet vazhdimisht.

1.7. Faktorët kritikë në arritjen e suksesit

Faktorët e mëposhtëm janë kritikë për zbatimin e suksesshëm të sigurisë së informacionit në mjedisin e sistemeve të IdentiTek:

- Politika e plotë e sigurisë së informacionit, objektivat dhe iniciativat që pasqyrojnë qartazi objektivat e IdentiTek.
- Qasja e sigurisë së informacionit që është konsistente me kulturën e IdentiTek
- Mbështetje shumë e dukshme nga Administratori i IdentiTek.
- Kuptimi solid i kërkesave të sigurisë dhe praktikave të menaxhimit të rreziqeve.
- Komunikimi efektiv i sigurisë së informacionit te të gjithë menaxherët, punonjësit, partnerët, klientët, furnizuesit dhe zhvilluesit e IdentiTek.
- Udhëzime mbi politikën e sigurisë së informacionit për të gjithë menaxherët, punonjësit, partnerët, klientët, furnizuesit dhe zhvilluesit e IdentiTek.
- Njohuritë dhe trajnimet mbi sigurinë e informacionit.
- Rishikimi dhe vlerësimi i vazhdueshëm i efektshmërisë dhe efiçencës të kontrolleve dhe mekanizmave të sigurisë së informacionit.
- Rregullimet në kohën e duhur, të kuadrit të sigurisë së informacionit duke adresuar mangësitë dhe duke reflektuar ndryshimet në objektivat e biznesit të IdentiTek sa herë që është e nevojshme.

1.8. Zhvillimi i politikave të IdentiTek

IdentiTek ka krijuar dhe menaxhon politika të sigurisë në këto fusha:

- Politika e Menaxhimit të Sigurisë (përfshirë deklaratat e politikës në lidhje me përdorimin e pranueshëm të burimeve dhe trajnimin e ndërgjegjësimit të sigurisë).
- Organizimin e Sigurisë
- Klasifikimin i Burimeve
- Sigurinë Fizike
- Sigurinë e Personelit
- Komunikimet dhe Operacionet (përfshirë politikat në lidhje me lidhjen në rrjet të partnerëve të biznesit).
- Kontrolli i Aksesit në Sisteme
- Zhvillimi dhe Mirëmbajtja e Sistemeve
- Reagimi ndaj Incidenteve
- Planifikimi i Vazhdimësisë së Biznesit
- Përmbushja e Rregullave
- Menaxhimi i Informacionit të Dokumentuar

Përgjegjës për krijimin e politikave të lartpërmendura janë përkatësisht:

- Departamenti i Sigurisë së Informacionit,
- Departamenti i Teknologjisë dhe Informacionit,
- Departamenti i Burimeve Njerëzore
- Departamenti i Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes
- Departamenti Ligjor
- Departamenti i Cilësisë dhe Standardeve

2. FUSHË-VEPRIMI DHE PËRKUFIZIMET

2.1. Fushëveprimi

Fushëveprimi përfshin politikat dhe standardet e IdentiTek për të mbrojtur të gjitha burimet e teknologjisë së informacionit dhe kompjuterike që aplikohen për punonjësit të cilët punojnë në sistemin qendror të IdentiTek dhe në vendet e regjistrimit/dorëzimit, duke përfshirë menaxherët dhe drejtuesit, si dhe kontraktorët e jashtëm. Çdo person që nuk është i mbuluar nga këto politika dhe standarde (p.sh, vizitorët) duhet të mbikëqyren nga një punonjës gjatë kohës që ndodhen në ambientet e Institucionit. Informacioni lidhur me këto politika si dhe zbatimi i tyre, duhet të jetë i disponueshëm për të gjithë stafin e prekur nga menaxheri i tyre përgjegjës.
Këto politika aplikohen për burimet e informacionit të IdentiTek, të cilat përfshijnë të gjitha pajisjet dhe "software" kompjuterik dhe të komunikacionit, sistemet e rrjetit, në pronësi, në qira ose të operuara nga Shoqëria, të dhënat e ruajtura aty, dhe të gjitha kompjuterët e jashtëm si stacionet e regjistrimit/dorëzimit të vendosura jashtë Sistemit Qendror, në zyra të ndryshme jashtë IdentiTek. Të njëjta politika aplikohen për të gjitha platformat (sistemet operative), sistemet kompjuterike dhe të gjitha aplikacionet (qoftë të zhvilluara brenda organizatës ose të blera nga palë të treta).

2.2. Termat dhe përkufizimet

Për qëllimet e këtij dokumenti, ju lutemi referohuni te përkufizimet dhe termat e listuar në seksionin Fjalori dhe Terminologjia e këtij dokumenti.

2.3. Siguria e Informacionit

Kjo është ruajtja e konfidencialitetit, integritetit dhe disponueshmërisë së informacionit.

- **Konfidencialiteti:** Informacioni të jetë i sigurt dhe përqasja të jetë vetëm për ata që janë autorizuar për të pasur akses.
- **Integriteti:** Mbrojtja e saktësisë dhe plotësisë së informacionit dhe metodave të përpunimit.
- **Disponueshmëria:** Përdoruesit e autorizuar të kenë akses në informacion dhe asetet e lidhura me të, kur kërkohet.

2.4. Vlerësimi i Riskut

Ky është vlerësimi i kërcënimeve ndaj sistemeve të informacionit dhe dobësive në këto sisteme.

2.5. Menaxhimi i Riskut

Ky është procesi i identifikimit, kontrollit dhe minimizimit ose eliminimit të rreziqeve të sigurisë që mund të ndikojnë në sistemet e informacionit.

3. STRUKTURA E KËTIJ STANDARDI

3.1. Klauzolat

Ky dokument ofron detajet e politikave dhe procedurave të përgjithshme të sigurisë për IdentiTek. Është një dokument në zhvillim që duhet të përditësohet dhe të referohet vazhdimisht.

3.2. Kategoritë Kryesore të Sigurisë

Standardi ISO/IEC 27001 përmban 14 seksione kryesore të sigurisë.
Kjo organizatë bazohet në versionin ISO 27001:2022:

- Politikat e Sigurisë së Informacionit
    - Drejtimi i menaxhimit për sigurinë e informacionit
- Organizimi i Sigurisë së Informacionit
    - Organizimi i brendshëm
    - Përdorimi i pajisjeve mobile dhe puna në distancë
- Siguria e Burimeve Njerëzore
    - Përpara punësimit
    - Gjatë punësimit
    - Shkarkimi ose ndryshimi i punës
- Menaxhimi i Aseteve
    - Përgjegjësia për asetet
    - Klasifikimi i informacionit
- Kontrolli i Hyrjeve
    - Kërkesat e biznesit për kontrollin e hyrjeve
    - Menaxhimi i hyrjeve të përdoruesve
    - Përgjegjësitë e përdoruesve
    - Kontrolli i hyrjeve në sistemet dhe aplikacionet
- Kriptografia

- Kontrollet kriptografike

- Siguria Fizike dhe Mirëmbajtja
  - Zonat e sigurta
  - Siguria e pajisjeve
- Siguria e Operacioneve
  - Procedurat dhe përgjegjësitë operative
  - Mbrojtja nga softuerët e dëmshëm
  - Back-up
  - Log-imet dhe monitorimet
  - Kontrolli i software-ëve operative
  - Menaxhimi i vulnerabiliteteve teknike
  - Konsideratat e auditimit të sistemeve të informacionit
- Siguria e Komunikimit
  - Menaxhimi i Sigurisë së Rrjetit
  - Transferimi i informacionit
- Prokurimi, Zhvillimi dhe Mirëmbajtja e Sistemeve
  - Kërkesat e sigurisë për sistemet e informacionit
  - Proceset dhe mbështetja e zhvillimit të sigurisë
  - Të dhënat e testimit
- Marrëdhëniet me Furnizuesit
  - Siguria e informacionit në marrëdhëniet me furnizuesit
  - Menaxhimi i ofrimit të shërbimeve nga furnizuesit
- Menaxhimi i Incidenteve të Sigurisë së Informacionit
  - Menaxhimi i incidenteve dhe përmirësimeve të sigurisë së informacionit
- Aspektet e Sigurisë së Informacionit të Menaxhimit të Vazhdueshmërisë së Biznesit
  - Qëndrueshmëria e sigurisë së informacionit
  - “Redundancy”

- Përputhshmëria
    - Përputhshmëria me kërkesat ligjore dhe kontraktuale

4. VLERËSIMI DHE TRAJTIMI I RREZIKUT

4.1. Vlerësimi i Rreziqeve të Sigurisë

Kërkesat për sigurinë e informacionit përcaktohen përmes një vlerësimi metodik të rreziqeve. Drejtuesit e IdentiTek balancojnë kostot që shoqërojnë zbatimin e kontrolleve dhe mekanizmave të sigurisë kundër dëmeve potenciale që mund të rezultojnë nga një dështim i sigurisë në sistemet e IdentiTek. Gjatë kryerjes së vlerësimeve të rreziqeve, konsiderohen të dhënat vijuese:

- Dëmi për shoqërinë si rezultat i një dështimi të sigurisë - duke konsideruar pasojat potenciale të humbjes së konfidencialitetit, integritetit dhe/ose disponueshmërisë së informacionit, të dhënave private të qytetarëve Shqiptarë.
- Shkalla e mundshme e një dështimi që mund të ndodhë për shkak të kërcënimeve dhe vulnerabiliteteve në mjedisin e sistemeve IdentiTek.

Pas një vlerësimi të plotë të rreziqeve, përcaktohen veprimet e përshtatshme dhe prioritetet për menaxhimin e rreziqeve të sigurisë së informacionit në mjedisin e sistemeve IdentiTek.

Rishikime periodike të rreziqeve të sigurisë dhe kontrolleve të mekanizmave të zbatuara duhet të kryhen një herë në vit për:

- Të përballuar ndryshimet në kërkesat dhe prioritetet e biznesit.
- Të konsideruar kërcënime dhe vulnerabilitete të reja që mund të ekzistojnë.
- Të konfirmuar që kontrollet dhe mekanizmat e sigurisë mbeten efektive dhe efikase.

4.2. Trajtimi i Rreziqeve të Sigurisë

Kjo kategori ka për qëllim zvogëlimin e rreziqeve, në përputhje të objektivave të shoqërisë. Për të zvogëluar rreziqet e identifikuara, duhet të ndërmerren përpjekje për trajtimin e tyre duke përdorur kontrollet administrative, teknike dhe fizike.

Kontrollet përfshijnë:

- Zbatimin e kontrolleve të përshtatshme për të shmangur, eliminuar ose zvogëluar rreziqet.
- Transferimin e disa rreziqeve tek palë të treta sipas nevojës (p.sh. përmes kompanive të sigurimit)
- Pranimin me vetëdije i disa rreziqeve
- Dokumentimin e zgjedhjeve për trajtimin e rreziqeve përfshire arsyet për to.

Trajtimi i rreziqeve duhet të marrë parasysh:

- Kërkesat ligjore-rregullore dhe ato që pasojnë si rrjedhojë e certifikimit sipas Standardeve Ndërkombëtare si ISO 27001;
- Objektivat e shoqërisë, kërkesat operacionale dhe kufizimet;
- Kostot e zbatimit dhe operimit në krahasim me rreziqet që po zvogëlohen.

5. POLITIKA E SIGURISË

5.1. Politika e Sigurisë së Informacionit

5.1.1. Dokumenti i Politikës së Sigurisë së Informacionit

Objektivi i këtij dokumenti është të ofrojë strategjinë e Drejtuesve të Shoqërisë dhe mbështetje për sigurinë e informacionit. Drejtuesit e shoqërisë duhet të vendosin një strategji të saktë dhe të tregojnë mbështetjen dhe angazhimin e tyre për sigurinë e informacionit nëpërmjet nxjerrjes dhe mirëmbajtjes së një politike të sigurisë së informacionit në IdentiTek.
Drejtuesit e Shoqërisë duhet të miratojnë një ose më shumë dokumente të politikës së sigurisë së informacionit, t'i publikojë dhe t'jua komunikojë ato, të gjithë punonjësve dhe palëve të jashtme të rëndësishme të përfshira. Kontrolli përfshin:

- Objektivat e përgjithshme të sigurisë së informacionit dhe fushën e veprimit, duke përfshirë deklaratën e qëllimit të drejtuesve të Shoqërisë, qëllimet e mbështetjes për sigurinë dhe parimet e sigurisë së informacionit;
- Renditjen e autoriteteve të identifikuara dhe kërkesave që kushtëzojnë ose kontrollojnë aktivitetet e sigurisë së informacionit, duke përfshirë një shpjegim ose renditje të politikave të sigurisë, parimeve, standardeve dhe kërkesave të përputhshmërisë me rëndësi për Shoqërinë;
- Kuadrin për vendosjen e kontrolleve dhe objektivave të tyre, duke përfshirë një strukturë për vlerësimin e rreziqeve “risk” dhe menaxhimin e tyre;
- Përcaktimet e përgjegjësive të përgjithshme dhe specifike për menaxhimin e sigurisë së informacionit;
- Referencat për dokumente që mbështesin ose nënvijëzojnë politikat.

Objektivi i sigurisë së informacionit është të sigurojë qëndrueshmërinë e aktiviteteve të Shoqërisë IdentiTek dhe të minimizojë rrezikun e dëmtimit duke parandaluar ngjarjet e sigurisë dhe ulur impaktin e tyre të mundshëm.

5.1.2. Rishikimi i Politikës së Sigurisë së Informacionit

Rregullat e mëposhtme kanë për qëllim të menaxhojnë zbatimin dhe zhvillimin e këtij dokumenti.

[POL_01] Përditësimi dhe Rishikimi i Politikës së Sigurisë

Menaxheri i Departamentit të Sigurisë së Informacionit në IdentiTek është përgjegjës për përditësimin vjetor të kësaj Politike të Sigurisë së Informacionit.

Menaxheri i Departamentit të Sigurisë së Informacionit në IdentiTek përkujdeset që Politika e Sigurisë së Informacionit të qëndrojë në përputhje dhe të sinkronizohet me zhvillimet kryesore të Sistemeve të Informacionit të IdentiTek dhe nevojat e kërkuara të sigurisë.

[POL_02] Miratimi i Politikës së Sigurisë

Çdo version i ri i Politikës së Sigurisë së Informacionit të IdentiTek miratohet nga Drejtuesit e Shoqërisë përpara se të aplikohet.

[POL_03] Politika e Sigurisë Shpërndarja / Publikimi

Politika e Sigurisë së Informacionit të IdentiTek është publikuar dhe është e disponueshme për:

- Të gjithë punonjësit e IdentiTek;
- Bashkëpunëtorët, furnizuesit, nën-kontraktorët në lidhje me Sistemet e Informacionit të IdentiTek. Shpërndarja e kësaj politike të sigurisë duhet të realizohet në përputhje me nevojat e identifikuara dhe pas nënshkrimit të një marrëveshjeje konfidencialiteti nga këta persona apo entitete.

Drejtori përkatës i Divizionit të Sistemeve të Informacionit në IdentiTek menaxhon shpërndarjen dhe publikimin.

[POL_04] Zbatimi dhe aplikimi i Politikës së Sigurisë

Menaxheri i Departamentit të Sigurisë së Informacionit në IdentiTek siguron ndjekjen e zbatimit të politikës së sigurisë në një proces të vazhdueshëm përmirësimi.

6. ORGANIZIMI I SIGURISË SË INFORMACIONIT

6.1. Organizimi i brendshëm

Qëllimi i këtij seksioni është menaxhimi i sigurisë së informacionit brenda strukturës administrative të IdentiTek.

6.1.1. Angazhimi i drejtuesve në Sigurinë e Informacionit

Një nga parimet themelore të menaxhimit të vazhdueshëm të sigurisë bazohet në nevojën për të përfshirë Drejtuesit më të lartë të Shoqërisë dhe të gjithë punonjësit. Përcaktimi dhe miratimi i drejtimeve që do ndiqen për sigurinë e informacionit brenda Shoqërisë nuk mund të optimizohet pa përfshirjen aktive të përgjegjësve të ndryshëm.

Organizimi i sigurisë bazohet në një punë bashkëpunuese mes përgjegjësve të ndryshëm dhe aktorëve të tjerë.

Administratori i Institucionit ose përfaqësuesi i tij drejtpërdrejtë.

Administratori miraton objektivat e kësaj politike sigurie dhe siguron alokimin e burimeve të nevojshme për zbatimin e saj.

6.1.2. Koordinimi i Sigurisë së Informacionit

Aktivitetet e sigurisë së informacionit koordinohen nga përfaqësues të ndryshëm të IdentiTek me role dhe detyra të përshtatshme. Ky koordinim bëhet nga Menaxheri i Departamentit të Sigurisë së Informacionit në IdentiTek nën udhëheqjen e Drejtorit të Divizionit të Sistemeve të Informacionit. Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek ka përgjegjësinë për të gjitha politikat dhe procedurat të sigurisë së informacionit.

"Përgjegjësia" përfshin përgjegjësinë për krijimin, mirëmbajtjen, vlerësimin dhe përputhshmërinë e zbatimit të të gjitha politikave të sigurisë.

Koordinimi i bërë nga Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek nën qeverisjen e Drejtorit të Divizionit të Sistemeve të Informacionit në IdentiTek kryhet kryesisht me:

- Menaxherin e Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes
- Drejtorin e Divizionit të Operacioneve të IdentiTek;
- Drejtorin e Departamentit të Teknologjisë dhe Informacionit të IdentiTek;
- Menaxherin e lartë të Sektorit të Sistemeve dhe Infrastrukturës IT
- Menaxherin e lartë të Sektorit të Sigurisë së Rrjetit Kompjuterik dhe Shërbimeve IT

- Drejtorin e Departamentit të Financave dhe Planifikimin Financiar;
- Menaxherin e Departamentit të Cilësisë dhe Standardeve;
- Menaxherin e Departamentit e Prodhimit të IdentiTek;
- Menaxherin e Departamentit të Burimeve Njerëzore të IdentiTek.

Drejtori i Divizionit të Sistemeve të Informacionit i IdentiTek ka këto përgjegjësi:

- Rishikimin dhe miratimin e politikës së sigurisë së informacionit dhe përgjegjësitë e përgjithshme;
- Vlerëson përshtatshmërinë dhe koordinon zbatimin e kontrolleve;
- Siguron që kontrollet e sigurisë së informacionit të zbatohen në përputhje me politikën e sigurisë së informacionit;
- Propozon metodologji dhe procese (p.sh. vlerësim të rreziqeve);
- Rishikon dhe monitoron incidentet e sigurisë së informacionit në të gjithë IdentiTek dhe propozon veprimet e përshtatshme;
- Identifikon ndryshimet e kërcënimeve dhe vulnerabiliteteve dhe propozon veprimet e përshtatshme;
- Promovon ndërgjegjësimin e sigurisë dhe trajnimin në të gjithë IdentiTek.

Drejtori i Divizionit të Sistemeve të Informacionit i IdentiTek:

- Miraton rolet dhe përgjegjësitë specifike për sigurinë e informacionit në të gjithë shoqërinë;
- Miraton metodologjitë dhe proceset specifike për sigurinë e informacionit, p.sh., vlerësimin e rreziqeve, sistemin e klasifikimit të sigurisë;
- Miraton dhe mbështet iniciativat për sigurinë e informacionit në të gjithë shoqërinë, p.sh., programin e ndërgjegjësimit të sigurisë;
- Koordinon që siguria është pjesë përbërëse e proceseve të planifikimit të sistemeve të informacionit; vlerëson përshtatshmërinë dhe koordinon zbatimin e kontrolleve specifike të sigurisë së informacionit për sistemet ose shërbimet e reja;
- Rishikon incidentet e sigurisë së informacionit;
- Promovon mbështetjen e biznesit për sigurinë e informacionit në të gjithë Shoqërinë.

6.1.3. Përcaktimi i Përgjegjësive të Sigurisë së Informacionit

Përcaktimi i përgjegjësive të sigurisë së informacionit bëhet duke u bazuar në strukturën administrative të ISMS e përshkruar si më poshtë.

Administratori i IdentiTek

Administratori miraton objektivat e kësaj politike të sigurisë dhe siguron përcaktimin e burimeve të nevojshme për zbatimin e saj (Management Commitment).

Drejtori i Divizionit të Sistemeve të Informacionit të IdentiTek;

Drejtori i Divizionit të Sistemeve të Informacionit IdentiTek është përgjegjës për menaxhimin e implementimit të sigurisë. Në bashkëpunim me Menaxherin e Departamentit të Sigurisë së Informacionit të IdentiTek dhe Menaxherin e Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes (por jo vetëm), ai/ajo ka misionin për të siguruar respektimin e konfidencialitetit, integritetit, disponueshmërisë së të dhënave ose informacionit të IdentiTek. Ai/ajo siguron zbatimin e të gjitha procedurave të kërkuara për të adresuar këto pika dhe ofron ndjekjen dhe menaxhimin e tyre.
Drejtori i Divizionit të Sistemeve të Informacionit të IdentiTek; është përgjegjës për monitorimin dhe ndjekjen e zbatimin Politikave të Sigurisë në Departamentet në:

- Departamentin e Teknologjisë dhe Informacionit të IdentiTek;
- Sektorin e Sistemeve dhe Infrastrukturës
- Sektorin e Sigurisë së Rrjetit Kompjuterik dhe Shërbimeve të IT.
- Departamentin e Sigurisë së Informacionit.

Drejtori i Departamentit të Financave dhe Planifikimin Financiar;

- Plotëson të gjitha detyrat administrative, financiare dhe fiskale sipas rregullave dhe ligjeve vendore, duke siguruar efikasitetin dhe transparencën e proceseve të biznesit;
- Mbështet ngushtë Administratorin e Shoqërisë gjatë procesit të komunikimit dhe negocimit me Autoritetet e Qeverisë për të gjitha çështjet; p.sh. përmirësimin e shërbimeve, shërbimet e reja, të gjitha çështjet financiare;
- Koordinon dhe harton planifikimin shumëvjeçar dhe buxhetin vjetor në përputhje me udhëzimet dhe në bashkëpunim me departamentet e tjera;
- Koordinon të gjitha aktivitetet me konsulentët dhe kontrolluesit e Kompanisë (ligjorë, tatimorë, etj.), me fokus në auditimet financiare dhe tatimore vjetore;
- Harton Planin e Biznesit të Kompanisë.

Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek

Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek është përgjegjës për monitorimin dhe ndjekjen e zbatimin në perimetrin e tij/saj të operacioneve, për:

- Përcaktimin, përditësimin dhe raportimin e hartës së rreziqeve të IT-së;
- Përcaktimin, përditësimin dhe publikimin e Politikes së Sigurisë së Sistemeve të Informacioneve IdentiTek ISSP (ky dokument);
- Koordinon që stafi IT-ja e IdentiTek të mbetet e përditësuar në terma të sigurisë.
- Përcaktimin dhe monitorimin e treguesve të sigurisë së IT-së (IT Security KPI) ;
- Drejtimin e proceseve për certifikatat e sigurisë, auditimet dhe inspektimet e brendshme dhe të jashtme të sigurisë;
- Monitorimin e ISMS;
- Siguron që incidentet e sigurisë së informacionit trajtohen në mënyrë të duhur, në mënyrën më të mirë për të ruajtur interesat e IdentiTek;
- Koordinon edukimin dhe trajnimin e punonjësve në temat e sigurisë së informacionit.

<u>Drejtori i Departamentit të Teknologjisë dhe Informacionit</u>

Drejtori i Departamentit të Teknologjisë dhe Informacionit të IdentiTek është përgjegjës për monitorimin dhe ndjekjen e zbatimin në perimetrin e tij të operacioneve, për:

- Kontrollet e sigurisë që vijnë nga dokumentet e përgjithshme të publikuara nga Drejtori i Divizionit të Sistemeve të Informacionit i IdentiTek;
- Kontrollet e sigurisë të përcaktuara brenda specifikimeve të produktit/projektit;
- Plane rimëkëmbjes dhe emergjencash të TI;

Drejtori i Departamentit të Teknologjisë dhe Informacionit të IdentiTek ka gjithashtu përgjegjësi:

- Për të informuar sistematikisht Menaxherin e Departamentit të Sigurisë së Informacionit të IdentiTek në lidhje me punët që mund të kenë ndikim në kontrollet e sigurisë, ose për të ndryshuar listën e rreziqeve;
- Për të inventarizuar asetet (aplikacionet, informacionin) për të cilat ai/ajo është zotërues dhe për ta mbajtur të përditësuar listën e këtyre aseteve, përfshirë klasifikimet e tyre;
- Për të raportuar menjëherë Menaxherit të Departamentit të Sigurisë së Informacionit të IdentiTek:
  - për çdo tentativë ndërhyrjeje ose sjellje që mund të kompromentojë sigurinë e këtyre sistemeve dhe që mund të vihet në dijeni gjatë kryerjes së detyrave;
  - për çdo incident të sigurisë.

Menaxheri i Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes

Menaxheri i Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes, ka për mision të implementojë dhe të kontrollojë zbatimin e sigurisë fizike. Menaxheri i Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes është veçanërisht përgjegjës për:

- Sigurimin e integritetit të ambienteve të IdentiTek dhe për kontrollin e personave që hyjnë në to;
- Garantimin e sigurisë fizike të pajisjeve dhe aseteve;
- Për menaxhimin e detyrave dhe rregullave që lidhen me sigurinë fizike gjatë ndërveprimeve me palët e treta ose kontraktorët;
- Për të marrë në konsideratë rreziqet kryesore të lidhura me mbrojtjen e infrastrukturës industriale (makina personalizimi etj.) për të siguruar trajtimin e këtyre rreziqeve (zbatimin e kontrolleve dhe mjetet e përshtatura për ti mbuluar këto rreziqe) dhe për të menaxhuar zbatimin e këtyre kontrolleve dhe mjeteve, në mënyrë që të ketë një menaxhim të vazhdueshëm të sigurisë fizike;
- Për të inventarizuar asetet për të cilat ai/ajo është përgjegjës dhe për të ruajtur një listë të përditësuar të këtyre aseteve, përfshirë klasifikimet e tyre.

Menaxheri i Departamentit të Burimeve Njerëzore të IdentiTek

Menaxheri i Departamentit të Burimeve Njerëzore të IdentiTek ka detyrën të sigurojë që departamenti i burimeve njerëzore të zbatojë të gjitha hapat dhe kontrollet e sigurisë të lidhura me punonjësit dhe të informojë Administratorin e IdentiTek për zbatimin e tyre.

Menaxheri i Burimeve Njerëzore të IdentiTek është përgjegjës për t'i dhënë çdo punonjësi të ri dokumentet e referuara të sigurisë (kontratën e punonjësit, marrëveshjen e konfidencialitetin, politikat, kodin e etikës).

Menaxheri i Departamentit të Burimeve Njerëzore të IdentiTek ruan një listë të përditësuar të punonjësve që i bashkohen apo i largohen IdentiTek dhe informon Menaxherin e Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes të IdentiTek, si edhe Drejtorin/Menaxherin përkatës të Linjës, të cilët më pas kanë përgjegjësinë për të informuar Menaxherin e Departamentit të Sigurisë së Informacionit të IdentiTek dhe Drejtorin e Departamentit të Teknologjisë së Informacionit të IdentiTek për dhënien apo heqjen e të drejtave të akseseve.

Menaxher i Cilësisë dhe Standardeve të IdentiTek

Menaxheri i Departamentit të Cilësisë dhe Standardeve ka për detyrë të vlerësojë nivelin e menaxhimit të operacioneve nga pikëpamja e përputhshmërisë me Standardin ISO 27001 dhe kërkesat e tij, si edhe të suportojë në procesin dhe konsolidimin e menaxhimit të riskut dhe ndërgjegjësimit.

Ai është përgjegjës për menaxhimin dhe standardizimin e informacionit të dokumentuar në përputhje me kërkesat e standardit ISO, si dhe mbikëqyrjen dhe rishikimet/kontrollet e implementuara përmes planit vjetor.

Në kuadër të Auditit të Brendshëm dhe të Jashtëm, ai mbështet me dokumentacionin dhe evidencat e kërkuara duke garantuar mirëmbajtjen dhe kontrollin periodik të:

- Obsolesencës së dokumentacionit.
- Përputhshmërisë së dokumentacionit me proceset reale.
- Mbështet kontrollet e implementuara dhe listuara në ISSP.

Ai/Ajo bashkëpunon ngushtësisht me gjithë stafin e përfshirë në certifikimin ISO dhe strukturat e brendshme duke propozuar kontrolle sigurie për të përmirësuar dhe forcuar sigurinë e informacionit në IdentiTek.

Menaxheri i Departamentit të Prodhimit të IdentiTek

Menaxheri i Departamentit të Prodhimit të IdentiTek është përgjegjës për menaxhimin e personalizimit dhe prodhimit të letërnjoftimeve elektronike, lejeve të qëndrimit dhe pasaportave biometrike për qytetarët Shqiptarë. Ky perimetër përfshin aplikacionet, informacionin konfidencial, trajtimet automatike ose manuale të informacionit.

Është përgjegjësi e Menaxherit të Departamentit të Prodhimit të IdentiTek që:

- Të inventarizojë asetet për të cilat ai/ajo është zotërues dhe për të ruajtur një listë të përditësuar të këtyre aseteve, përfshirë klasifikimet e tyre.
- Identifikojë nevojat për sigurinë e aplikacioneve ose informacionit të cilin ai/ajo zotëron si dhe rreziqet përkatëse, dhe siguron në bashkëpunim me Drejtorin e Divizionit të Operacioneve të IdentiTek dhe Drejtorin e Departamentit të Teknologjisë dhe Informacionit të IdentiTek, që kontrollet e duhura të sigurisë përcaktohen dhe zbatohen në mënyrë të përshtatshme.

Drejtori Hierarkik ose Menaxheri i Linjës

Drejtori Hierarkik/Menaxheri i Linjës, përcakton personat përgjegjës për të mbikëqyrur një ose më shumë punonjës (Team Leader).

Drejtori Hierarkik/Menaxheri i Linjës ka rol që të sensibilizojë punonjësit për çështjet e sigurisë.

Ai/ajo është gjithashtu përgjegjës për kërkesat e qasjes në sisteme (stacionet e punës) të punonjësve nën përgjegjësinë e tij/saj dhe i rishikon ato në mënyrë periodike.

Përdoruesi Fundor

Përdoruesi fundor përcakton çdo person që ka qasje në sistemin e Teknologjisë së Informacionit të IdentiTek. Ky person mund të jetë një punonjës i IdentiTek, një nënkontraktor në rastet kur mund të nevojitet ndërhyrja nga "prodhuesi i sistemeve" për mirëmbajtje apo zgjidhje problematikash apo incidentesh.

Përdoruesi fundor respekton rregullat e sigurisë të aplikueshme dhe informon eprorin e tij (ose të deleguarin) dhe Departamentin e Teknologjisë dhe Informacionit të IdentiTek në rast të kontrollit të pamjaftueshëm ose dështimit të kontrollit të sigurisë.

6.1.4. Ndryshimet në pajisjet e përpunimit të informacionit

IdentiTek ka përcaktuar një proces autorizimi për menaxhimin e ndryshimeve në pajisjet e përpunimit të informacionit ose të drejtat e përdorimit në to në përputhje me procesin e menaxhimit të ndryshimeve.

Kontrolle të tilla si:

- Pajisje të reja ose për pajisje ekzistuese që janë ndryshuar kanë miratimin formal të Drejtuesit hierarkik të përdoruesit, që autorizon qëllimin dhe përdorimin e tyre. Gjithashtu, duhet të merret miratimi nga Drejtori Hierarkik i cili është përgjegjës për mirëmbajtjen e mjedisit lokal të sigurisë së sistemit të informacionit, për të siguruar që të përmbushen të gjitha politikat dhe kërkesat e sigurisë relevante.

6.1.5. Kontakti me Autoritetet

[CAUT_01] Marrëdhënia me autoritetet gjyqësore

Administratori i IdentiTek është përgjegjës për të komunikuar me autoritetet gjyqësore (policinë, drejtësinë, qeverinë) në çështje të sigurisë, veçanërisht ato të lidhura me krimin kompjuterik të parashikuara në Legjislacionin e Republikës së Shqipërisë.

Drejtori i Divizionit të Operacioneve të IdentiTek, Drejtori i Divizionit të Sistemeve të Informacionit në IdentiTek, Drejtori i Departamentit të Teknologjisë së Informacionit të IdentiTek dhe ekspertët teknikë ofrojnë ndihmë nëse është e nevojshme.

6.1.6. Kontakti me Grupet e Interesit të Veçantë

Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek mund të jetë në kontakt me Departamentet e Sigurisë të Palëve të Treta me të cilat Shoqëria ka marrëveshje për mirëmbajtje të sistemeve (për shembull Idemia, Splunk, Trellix etj.) në rast se është e nevojshme për sigurinë e sistemeve të IT-së.

Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek duhet të jetë në kontakt për Raportimin e incidenteve kibernetike pranë AKSK.

6.1.7. Siguria e Informacionit në Menaxhimin e Projekteve

[PRMGM_01] Siguria e Informacionit në Menaxhimin e Projekteve

Siguria e informacionit duhet të integrohet që në fazën e parë të konceptimit të një projekti në metodën e menaxhimit të projekteve të shoqërisë IdentiTek, për të siguruar që rreziqet e sigurisë së informacionit identifikohen dhe adresohen si pjesë e projektit. Metodologjia duhet të sigurojë që objektivat e sigurisë së informacionit përfshihen në objektivat e projektit dhe që një vlerësim i rreziqeve të sigurisë së informacionit zhvillohet në një fazë të hershme të projektit për të identifikuar kontrollet e nevojshme.

6.1.8. Rishqyrtimi i Pavarur i Sigurisë së Informacionit

Përqasja e IdentiTek, është të vlerësohet në mënyrë të pavarur një herë në vit menaxhimi i sigurisë së informacionit dhe implementimi i saj, dhe gjithashtu në rastin e ndryshimeve të konsiderueshme në strukturën e brendshme, mjedisin e jashtëm apo ndryshime legjislative.

6.2. Puna kompjuterike në distancë

6.2.1. Puna kompjuterike në distancë

[NOMAD_01] Lidhja në distancë (mobile access)

Autorizimi për përdorimin e aksesit të lëvizshëm është i kushtëzuar nga një kërkesë formale dhe të motivuar, e miratuar nga përgjegjësi i departamentit dhe aprovuar nga Drejtori i Divizionit të Sistemeve të Informacionit në IdentiTek.

[NOMAD_02] Kontrollet e Sigurisë të Instaluara

Në çdo laptop, janë të instaluar automatikisht kontrollet e sigurisë të mëposhtme:

- Antivirus / anti-spam
- Program kodimi/ nënshkrim i skedarëve
- Firewall / HIPS (Sistem parandalimi i hyrjes së paautorizuar)
- Fshirja e sigurtë e skedarëve.

Bazuar në nevojat e identifikuara dhe të dhënat e trajtuara, mund të sigurohen edhe mjetet tjera për punonjësin (autentifikim i thelluar për lidhjen e laptopit, mjet për lidhjen e sigurt - VPN, mjet për kontrollin e lidhjeve të dyfishta (single session).

[NOMAD_03] Kthimi dhe rishpërndarja

Në rast ndryshimi të përdoruesit të një laptopi të lëvizshëm, laptopi ristrukturohet kur kthehet në fund të misionit. HDD fshihen dhe tokenat ri-incializohen.

6.2.2. Telepuna

[NOMAD_04] Lidhjet e Laptopëve

Lidhjet në distancë përdorin një mekanizëm autentifikimi të thelluar.

[NOMAD_05] Punësimi i Lëvizshëm dhe përdorimi i laptopëve jashtë IdentiTek

Punësimi i lëvizshëm dhe përdorimi i laptopëve jashtë IdentiTek kërkon që përdorimi i tyre të garantojë sigurinë e të dhënave të kompanisë dhe të mos kompromentojë sistemin e IT-së të IdentiTek.

7. SIGURIA E BURIMEVE NJERËZORE

Politika e Sigurisë së Burimeve Njerëzore zbatohet për të gjithë punonjësit e IdentiTek-ut, përfshirë menaxherët, drejtuesit dhe kontraktorët e jashtëm.

Termi "anëtar i stafit" përfshin çdo person që ka një kontratë pune me IdentiTek: punonjës, praktikant.

Termi "nën-kontraktor" përfshin çdo person që nuk është punonjës i IdentiTek, por punon për IdentiTek-un dhe i përket një kompanie në marrëdhënie kontraktuale me IdentiTek.

Termi "person" përfaqëson një anëtar të stafit ose një nën-kontraktor.

7.1. Përpara Punësimit

7.1.1. Rolet dhe Përgjegjësitë

[HRM_01] Identifikimi i sigurisë gjatë përzgjedhjes së kandidatit

Gjatë fazës së para-punësimit, verifikohet aftësia e kanditatit për të përmbushur rregullat e sigurisë dhe për të patur një sjellje në përputhje me politikat e brendshme të IDENTITEK dhe aftësinë për të respektuar udhëzimet e sigurisë.

[HRM_02] Komunikimi me personelin

Të drejtat, detyrat dhe përgjegjësitë e lidhura me çdo funksion në lidhje me sigurinë e sistemit të informacionit komunikohen tek çdo punonjës i Shoqërisë gjatë fillimit të punës ose gjatë çdo funksioni të ri (p.sh.: ndryshimi i pozicionit të punës).

Forma e krijimit/modifikimit të llogarisë së përdoruesit i jepet punonjësit nga Drejtori/Përgjegjësi Hierarkik. Dokumentet që përfshihen në kontratën e punës së punonjësit, kodin e etikës, marrëveshjen e konfidencialitetit të ofruar çdo punonjësi, ofrojnë informacion lidhur me udhëzimet e sigurisë që duhet të respektohen gjatë kryerjes së detyrave që ai/ajo zhvillon brenda organizatës dhe jepet nga Departamenti i Burimeve Njerëzore.

Trajnimi për këtë informacion kryhet nga departamenti i Burimeve Njerëzore (BNJ). Përgjegjësia për informimin dhe komunikimin me nën kontraktorët bie mbi çdo Drejtor/Menaxher që ka kërkuar shërbime nga kontrakori.

7.1.2. Shqyrtimi i punonjësve

[HRM_03] Procesi i Shqyrtimit

Punonjësit e IdentiTek që do të kenë akses në sistemet e informacionit që kalojnë në një proces kontrolli për të kaluarën e tyre (background-check). Ky proces kontrolli përfshin verifikimin e personave dhe marrjen e dokumenteve nga Gjykata apo Prokuroria që të verifikojnë statusin (i/e

dënuar / padënuar) e punonjësit. Këto verifikime realizohen nga Departamenti i Burimeve Njerëzore (BNJ). Kontraktorët që do të kenë akses fizik në sistemet e informacionit verifikohen nga Menaxheri i Departamentit të Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes dhe për akses logjik nga Menaxheri i Departamentit të Sigurisë së Informacionit.

7.1.3. Termat dhe Kushtet e Punësimit

[HRM_04] Përgjegjësitë e Përgjithshme

Forma e llogarisë së përdoruesit e dorëzuar nga Drejtori/Përgjegjësi Hierarkik, kodi i etikës dhe kontrata e punësimit që përmban përdorimin e sistemit dhe sigurinë e sistemit të informacionit të IdentiTek përshkruajnë nivelin e aksesit që i takojnë çdo përdoruesi të sistemit të informacionit për qëllime sigurie:

- Rregullat e përdorimit të mjeteve (kompjuter ose stacioni i punës mobil) dhe shërbimeve të përgjithshme (sistemi i postës elektronike, Intraneti, ...) të ofruara për secilin përdorues;
- Përgjegjësitë e përdoruesit në lidhje me sigurinë.

[HRM_05] Përgjegjësitë specifike dhe rolet e besuara.

Çdo Drejtor, Menaxher është përgjegjës për të përcaktuar sensivitetin dhe kërkesat për çdo rol brenda departamentit të tij/saj dhe për të identifikuar punët që do të kryhen.

Për çdo punë ose përdorues të privilegjuar, një deklaratë e politikës specifike përcakton pikat që shtohen në dokumentin që përshkruan përgjegjësitë e përgjithshme:

- Aktivitetet sensitive të prekura dhe kontrollet specifike.
- Aktivitetet sensitive dhe rregullat për t'u ndjekur.
- Dispozitat specifike (pikat për monitorimin, raportimin e ngjarjeve, ...).

[HRM_06] Marrëveshje konfidencialiteti

Marrëveshja e konfidencialitetit përfshihet në çdo kontratë mes IdentiTek dhe çdo person fizik që do të punojë për IdentiTek-un (punonjës). Çdo anëtar i personelit të IdentiTek zotohet për të respektuar këtë marrëveshje konfidencialiteti sapo fillon punën brenda Institucionit.

Persona të jashtëm (nën-kontraktorë, furnizues) që do të punojnë në ambiente të IdentiTek, nën përgjegjësinë e Departamentit të Sigurisë, nënshkruajnë një Marrëveshje Konfidencialiteti.

Proceset e Burimeve Njerëzore që lidhen me:

- Ndërgjegjësimi dhe trajnimi për sigurinë e informacionit;
- Procesi disiplinor;

- Përfundimi i punësimit;
- Kthimi i aseteve;
- Aksesi kur punonjësi nuk është më në strukturën e institucionit

Detajohen specifikisht në Procedurën e Burimeve Njerëzore ADM-BNJ-002 dhe në formularin përkatës.

8. MENAXHIMI I ASETEVE

Qëllimi i menaxhimit të aseteve është të implementojë dhe të ndihmojë në një mbrojtje të përshtatshme të aseteve sensitive të IdentiTek.

8.1. Përgjegjësia për Asetet

8.1.1. Inventari i Aseteve

Koncepti i "aseteve sensitive" përfshin çdo aset që nëse kompromentohet, ndryshohet, merret pa leje, ose shkatërrohet, mund të sjellë dëme serioze për IdentiTek.

[ASM_01] Identifikimi dhe Inventari i Aseteve Sensitive

Asetet sensitive që përfshihen në Sistemin e Informacionit (informacioni ose të dhënat, pasuritë softuerike, pasuritë fizike, shërbimet, dhe të tjera) identifikohen dhe inventarizohen. Për çdo aset dokumentohet: nivelin e klasifikimit të tij, punonjësi që e ka në pronësi, mbajtësin ose personat që kanë akses në të (për të dhënat), si dhe kërkesat rregullatore dhe kontraktuale që aplikohen për këtë aset.

[ASM_05] Sensitiviteti i aseteve mbështetëse

Sensitiviteti i aseteve mbështetëse përcaktohet nga nevoja më e lartë për sigurinë e konfidencialitetit, integritetit, dhe disponueshmërisë (Ref 8.2.1) të procesit të biznesit ose asetet e informacionit që i përdor ato.

[ASM_04] Etiketimi i Pajisjeve Fizike

Çdo pajisje harduerike (përveç komponentëve të brendshëm) identifikohet me një etiketë që nuk fshihet lehtë dhe është në inventar.

8.1.2. Pronësia e Aseteve

[ASM_02] Zotërimi dhe përgjegjësitë e aseteve sensitive

Çdo aset sensitiv është nën pronësinë e një punonjësi i cili ka përgjegjësinë për t'i klasifikuar saktë dhe për të kryer rregullisht një shqyrtim të nevojave të aksesit mbi aset.

8.1.3. Përdorimi i pranueshëm i Aseteve (Acceptable use of assets)

[ASM_03] Përdorimi i aseteve sensitive

Përdoruesit janë të informuar për rëndësinë e mbrojtjes së aseteve sensitive dhe janë të ndërgjegjshëm për kërkesat e sigurisë.

Çdo person, punonjës i IdentiTek ose nënkontraktues, është përgjegjës për përdorimin që bën me asetet dhe duhet të jetë në përputhje me rregullat e duhura të përdorimit për çdo nivel/kriter sigurie.

Çdo shkelje e këtyre rregullave të përdorimit mund të rezultojë në procese disiplinore/penale. Çdo parregullsi duhet të raportohet.

8.2. Klasifikimi i Informacionit

8.2.1. Udhëzimet e Klasifikimit

[CLG_01] Udhëzimet e Klasifikimit

Udhëzimet e klasifikimit përcaktohen për ti dhënë prioritet niveleve të mbrojtjes dhe për të menaxhuar asetet në përputhje me nevojat e identifikuara të sigurisë.

Këto udhëzime për klasifikim përdorin shkallë të sensitivitetit bazuar në kriteret e konfidencialitetit, integritetit dhe disponueshmërisë.

Nivelet e klasifikimit janë: (Publik, i Brendshëm, Sensitiv)

Klasifikimi i aseteve bazuar në sensitivitetin e tyre është për efekt të brendshëm klasifikimi dhe në përputhshmëri me Standardin ISO.

[CLG_02] Shkalla e Konfidencialitetit

Vlerësimi i konfidencialitetit bazohet në nevojën potenciale për ruajtjen e informacionit. Shkon nga 0 (pa nevojë për siguri) deri në 3 (nevojë shumë e rëndësishme). Sensitiviteti karakterizohet kështu nga një vlerë që përfaqëson nevojën e konfidencialitetit të asetit për të cilin është fjala.

Tabela 1 Shkalla e Konfidencialitetit

Niveli	Përshkrimi
0	Informacioni Publik mund të shpërndahet lirshëm jashtë IdentiTek. Për shembull, informacioni mund të publikohet në internet.
1	Informacioni ose të dhënat e brendshme mund të shpërndahen lirisht brenda IdentiTek, por nuk mund të shpërndahen jashtë IdentiTek. Kontrolli opsional (një zotërues mund të dërgojë informacionin të një palë e tretë duke justifikuar nevojën për ta ditur).
2	Informacioni ose të dhënat të një rëndësie të veçantë, për të cilin shpërndarja është e kufizuar të një grup i kufizuar i njerëzve që kanë nevojë të dinë, ose për të cilin zbulimi do të sillte dëme për shoqërinë, pa ndikuar në qëndrueshmërinë e shoqërinë.

3	Informacioni ose të dhënat sensitive, për të cilin shpërndarja është e kufizuar të një grup shumë i kufizuar i njerëzve që kanë nevojë të dinë, dhe për të cilin zbulimi do të sillte dëme të rënda për shoqërinë dhe do të ndikonte në qëndrueshmërinë e shoqërisë.

[CLG_03] Shkalla e Integritetit

Vlerësimi i integritetit bazohet në nevojën potenciale për garantimin e plotësisë së informacionit. Shkon nga 0 (pa nevojë për siguri) deri në 3 (nevojë shumë e rëndësishme). Sensitiviteti karakterizohet kështu nga një vlerë që përfaqëson nevojën për integritet të asetit për të cilin është fjala.

Tabela 2 Shkalla e Integritetit

Niveli	Përshkrimi
0	Humbja e integritetit të informacionit nuk ka pasoja të rëndësishme. Nuk nevojitet integritet i të dhënave.
1	Humbja e integritetit mund të ketë pasoja të vogla, pa shqetësime të mëdha. Humbja e integritetit është e pranueshme, por duhet të zbulohet. Të dhënat e shkëmbyera kërkojnë një llogaritje të thjeshtë të integritetit (lloji i kontrollit të integritetit, si checksum).
2	Humbja e integritetit mund të ketë pasoja të rënda, por të kufizuara në një perimetër të ngushtë. Humbja e integritetit është e pranueshme, por të dhënat duhet të rindërtohen. Të dhënat e shkëmbyera kërkojnë një llogaritje të fortë të integritetit (funksion hash si SHA-256).
3	Humbja e integritetit mund të ketë pasoja shumë të rënda dhe të ndikojë në nivelin e shoqërisë. Humbja e integritetit nuk tolerohet. Të dhënat e shkëmbyera duhet të nënshkruhen elektronikisht.

[CLG_04] Shkalla e Disponueshmërisë

Vlerësimi i Disponueshmërisë bazohet në nevojën potenciale për të pasur përqasje në informacion apo sistem. Shkon nga 0 (pa nevojë për disponueshmëri) deri në 3 (nevojë shumë e rëndësishme). Sensitiviteti karakterizohet kështu nga një vlerë që përfaqëson nevojën për disponueshmëri të asetit.

Tabela 3 Shkalla e Disponueshmërisë

Niveli	Përshkrimi
0	Mungesa e resurseve ose aplikacioneve për 5 ditë është e pranueshme.
1	Mungesa e resurseve ose aplikacioneve për 2 ditë është e pranueshme.
2	Mungesa e resurseve ose aplikacioneve për 1 ditë është e pranueshme.
3	Mungesa e resurseve ose aplikacioneve nuk mund të tejkalojë 0,5 ditë.

[CLG_05] Rishikimi Periodik i Klasifikimit

Një proces për të rishikuar periodikisht klasifikimin është përcaktuar në mënyrë që të ruhen kontrollet e sigurisë në përputhje me ndjeshmërinë e informacionit dhe për të ndjekur zhvillimin e tyre.

8.2.2. Etiketimi dhe Menaxhimi i Informacionit

[CLG_06] Etiketimi i Informacionit

Asetet sensitive etiketohen bazuar në sensivitetin e tyre për konfidencialitetin, ashtu si është përcaktuar në [CLG_02]. Kjo etiketë aplikohet për informacionin, për sistemet e tyre elektronikë (skedarët) si dhe dokumentet e printuara që përmbajnë këtë informacion.

Çdo informacion i pa etiketuar konsiderohet si i brendshëm.

[INL_04] Ruajtja e informacionit sensitiv në media të lëvizshme "removable/mobile".

Në momentin që ruhen në një mjet të lëvizshëm "removable ose mobile", informacioni konfidencial ose sekret duhet të kodohet (përveç atyre të përdorura për back-up e IT-së që ruhet në ambiente fizike të sigurta).

[INL_05] Ruajtja e informacionit sensitiv

Informacioni sensitiv në terma të disponueshmërisë, që është i nevojshëm për vazhdimësinë e biznesit pas një ngjarje madhore, katastrofe natyrore (zjarr, përmbytje, etj.) ruhet në një vend të sigurt, duke siguruar mbrojtjen e tij në integritet dhe disponueshmëri në përputhje me planifikimin e vazhdueshmërisë së biznesit.

8.2.3. Menaxhimi i Informacionit

[INL_01] Menaxhimi i Informacionit

Asetet sensitive i nënshtrohen rregullave për menaxhim, ruajtje, transmetim dhe shkatërrim. Këto rregulla përditësohen dhe mirëmbahen rregullisht në përputhje me planin e klasifikimit.

8.3. Menaxhimi i Mediave të Jashtme (USB, HDD etj.)

8.3.1. Menaxhimi i Aseteve

[INL_03] Përdorimi i mediave të jashtme të ruajtjes

Përdoruesit e pajisjeve ku ruhen të dhënat janë të ndërgjegjësuar për riskun e lidhur me këto mjete në terma të zbërthimit të informacionit. Informacioni i ruajtur në media të jashtme është gjithmonë i koduar. Duhet të përdoren vetëm media të identifikuara dhe të menaxhuara nga IdentiTek. Fshirja e të dhënave të ruajtura në këto media është përgjegjësi e përdoruesit. Mjetet për fshirjen e sigurtë ofrohen nga Departamenti i Teknologjisë dhe Informacionit të IdentiTek.

8.3.2. Shkatërrimi i Mediave

[INL_02] Mjetet e ruajtjes dhe shkatërrimit

IdentiTek ju ofron përdoruesve sisteme për kodimin e të dhënave dhe gjithashtu mjetet logjike për fshirje të sigurt dhe fizike (si çekan, trapan) të nevojshme për shkatërrimin e mediave të lëvizshme.

[INL_07] Shkatërrimi i Sigurt i Medias

Mediat (e lëvizshme) elektronike duhet të shkatërrohen në mënyrë të sigurt përmes grirjes (shredding). Mediat e të dhënave (disketë, tape, etj.), kartat dhe komponentët elektronikë sensitivë duhet të shpohen ose të thyhen. Në rastin e shkatërrimit të sigurt nga një palë e tretë, identiteti i palës së tretë duhet të vërtetohet nga Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek dhe një dëshmi për shkatërrim të sigurt duhet të jepet gjithmonë.

8.3.3. Transferimi i Medias Fizike

[INL_06] Transferimi Informacionit Sensitiv

Transmetimi fizik i mediave, pajisjeve ose dokumenteve përdor një mbrojtje të përshtatshme, si përdorimi i kontenierëve të mbyllur, dorëzimi me dorë ose paketimi i sigurtë dhe i pa manipulueshëm.

9. KONTROLLI I AKSESIT

9.1. Kërkesat e biznesit për kontrollin e aksesit

9.1.1. Politika e Kontrollit të Aksesit

[ACCP_01] Menaxhimi i të drejtave të alokuara të biznesit

Politika e kontrollit të aksesit në fuqi ka për qëllim të alokojë të drejtat e aksesit bazuar në kërkesat operacionale të proceseve të ndryshme të biznesit. Llojet e profileve përcaktohen dhe identifikohen të drejtat e aksesit të nevojshme për përdorim.

Të drejtat e alokuara kufizohen bazuar në kërkesat për kryerjen e detyrave në përgjegjësi të personit që ka profilin përkatës.

Lista e të drejtave të alokuara duhet të qëndroje e përditësuar dhe rishikohet periodikisht.

9.2. Menaxhimi i aksesit të përdoruesit

[ACCP_02] Procedura e menaxhimit dhe krijimit të të drejtave dhe aksesit

Për menaxhimin e autorizimeve ka një politikë dhe një procedurë. Procedura përfshin krijimin, ndryshimin dhe fshirjen e llogarive dhe të drejtave të lidhura me profilin e alokuar të përdoruesit.

Aksesi dhe rishikimet e të drejtave të aksesit në kasaforta janë të menaxhuara nga Menaxheri i Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes në IdentiTek.

[ACCP _03] Kërkesat në lidhje me krijimin apo modifikimet e të drejtat e aksesit

Për punonjësit e IdentiTek-ut, departamenti i Burimeve Njerëzore dhe menaxherët hierarkik janë përgjegjës për të aktivizuar procedurën në lidhje me ndryshimet e situatës së përdoruesve të brendshëm (punësim, ndryshime gjatë punës, largim).

[ACCP_04] Vlerësimi i kërkesave lidhur me ndryshimet e të drejtat e aksesit

Kjo është përgjegjësi e Drejtorëve/Menaxherëve të Departamenteve hierarkik të punonjësve dhe Menaxherit të Departamentit të Sigurisë së Informacionit të IdentiTek-ut për të validuar çdo kërkesë para se të caktohen të drejtat.

[ACCP_05] Zbatimi i parimit të ndarjes së detyrave.

Validimet e kërkesave për autorizime dhe të drejtave të aksesit bëhen në përputhje me parimin e ndarjes së detyrave (Ref 12.1.4).

Për këtë, TI dhe departamentet respektive mbajnë një dokument që lejon të përcaktohet, për çdo kërkesë, nëse ajo është e përputhur me të drejtat e tjera të aksesit që tashmë janë të caktuara për personat e përfshirë.

9.2.1. Regjistrimi i përdoruesit

[USRE_01] Identifikimi dhe autentifikimi

Përdoruesit e sistemit të IdentiTek identifikohen individualisht, si përdorues të sistemit. Çdo përdorues i sistemeve është i lidhur me informacione të autentifikimit (p.sh., fjalëkalim) në përputhshmëri me kërkesat e përcaktuara nga Shoqëria.

[USRE _02] Gjurmimi aksesit

Të gjitha akseset në të dhënat sensitive dhe funksionet kritike gjurmohen dhe analizohen dhe kontrollohen periodikisht. Regjistri i auditimit ose log-eve ruhen dhe mbahen në mënyrë të sigurt për një kohë të mjaftueshme për t'iu përgjigjur nevojave operacionale dhe për të përmbushur kërkesat rregullatore.

[USRE _03] Menaxhimi i llogarisë

Llogaritë individuale që nuk janë përdorur për 30 ditë çaktivizohen automatikisht. Kjo vlen edhe për llogaritë e reja që nuk kanë të paktën një lidhje të parë 3 ditë pas krijimit të tyre. Llogaritë e personave që janë larguar nga IdentiTek-u çaktivizohen.

[USRE _04] Karakteristikat e llogarisë

Çdo llogari mundëson identifikimin e titullarit të saj. Identifikuesit përputhen me kodifikimin e përcaktuar në politikën e Menaxhimit të Llogarisë dhe Fjalëkalimit të IdentiTek, dhe në Politikën e Menaxhimit të Llogarisë të Përdoruesit të IdentiTek.

9.2.2. Menaxhimi i Privilegjeve

[PRIVM_01] Menaxhimi i llogarive të privilegjuara.

Llogaritë e privilegjuara dhe të drejtat e alokuara për këto llogari janë të menaxhuara po ashtu si llogaritë e tjera. Ato janë të rezervuara për administratorë dhe operatorë. Një listë e shkruar e administratorëve dhe operatorëve që kanë akses në llogaritë e privilegjuara ekziston dhe mbahet e përditësuar. Për llogaritë e privilegjuara të përbashkëta, kjo listë tregon përgjegjësin e identifikuar dhe listën e personave që kanë akses në këtë llogari.

[PRIVM _02] Menaxhimi i llogarive të përbashkëta, shërbimi ose gjenerik

Në këtë kategori llogarish përfshihen llogaritë si "root" në Unix/Linux ose "administrator" në Windows, llogaritë e dedikuara për menaxhimin e softuerëve, etj. Përdorimi i këtyre llogarive kërkohet për të kryer operacione të veçanta të administrimit dhe monitorimit të sistemeve.

Çdo llogari duhet të ketë një person përgjegjës të identifikuar.

Përgjegjësi ka përgjegjësinë për menaxhimin e fjalëkalimit të llogarisë.

Përdorimi i llogarive të privilegjuara të përbashkëta kufizohet vetëm për detyrat e nevojshme që lidhen me administrimin e sistemeve. Për gjithë rastet e tjera duhet të përdoren llogaritë nominative (personale) në sisteme.

Nëse një llogari e sistemit duhet të përdoret nga një person tjetër përveç përgjegjësit ose një përdorues të akredituar, përdorimi duhet të bëhet në prani të përgjegjësit të llogarisë ose një personi të kualifikuar që përfaqëson përgjegjësin. Pas këtij përdorimi, fjalëkalimi ndryshohet nga ky person pa nevojën për të ndryshuar rregullat e ruajtjes së fjalëkalimit për të evituar ndërprerjet në prodhim.

[PRIVM _03] Menaxhimi i llogarive personale të sistemit

Llogaritë personale të sistemit janë llogari nominative të privilegjuara me të drejta të barabarta me llogaritë e sistemit që zëvendësojnë (root ose administrator etj.).

Llogaritë personale të sistemit krijohen për çdo person që justifikon përdorimin e një llogarie të privilegjuar. Ato ndahen (segregohen) nga llogaritë administrative ose aplikative të zotëruesve të tyre.

[PRIVM _04] Menaxhimi i llogarive të sistemit të palëve të treta

Këto janë llogari të dedikuara për instalimin ose mirëmbajtjen e pajisjeve dhe softuerëve.

Llogaritë që përdoren vetëm për instalimin e produkteve fshihen, ose të paktën çaktivizohen, kur instalimi përfundon.

Llogaritë që përdoren vetëm për mirëmbajtjen çaktivizohen jashtë operacioneve të mirëmbajtjes ose fjalëkalimet e tyre ndryshohen në fund të operacioneve të mirëmbajtjes.

9.2.3. Menaxhimi i fjalëkalimit të përdoruesit

[UPMA_01] Karakteristikat e fjalëkalimit

Fjalëkalimet duhet të përputhen me rregullat e përcaktuara në Politikën Menaxhimi i Llogarisë dhe Fjalëkalimit në ISMS të IdentiTek.

Fjalëkalimet duhet të mbrohen (konfidencialitet).

[UPMA_02] Autentifikimi me llogari të larta të privilegjuara nominative

Fjalëkalimet ndryshohen:

- Çdo 90 ditë.
- Pas ndërhyrjeve të mirëmbajtjes ose përdorimit të përkohshëm të llogarisë nga një palë e tretë.
- Në momentin që një person nuk bën më pjesë në listën e përdoruesve të autorizuar.

Kontrollet e posaçme të sigurisë mundësojnë konfidencialitetin e kodeve të fshehta që transmetohen në rrjet (për shembull: përdorimi i protokolleve të sigurta (ssh, sftp), administrimin e izoluar të rrjetit (segregim).

Kontrollet e posaçme të sigurisë mundësojnë disponueshmërinë e fjalëkalimeve të llogarive të privilegjuara (vendosur në një zarf të kodifikuar (tamper-proof envelope) dhe ruajtja në një vend të sigurt).

9.2.4. Rishikimi i të Drejtave të Aksesit të Përdoruesve.

[RUAR_01] Ndryshimet e përshtatshmërive dhe të drejtave të aksesit

Rishikimet e formalizuara të të drejtave të aksesit me qëllim heqjen e të drejtave të padëshiruara të aksesit kryhen periodikisht.

Ato kryhen nga Departamenti i Sigurisë së Informacionit të IdentiTek.

Një raport jepet sistematikisht:

- Drejtorit të Divizionit të Sistemeve të Informacionit në IdentiTek,
- Menaxherit të Departamentit të Sigurisë së Informacionit të IdentiTek,
- Drejtorit të Departamentit të Teknologjisë së Informacionit të IdentiTek.

9.3. Përgjegjësitë e Përdoruesit

9.3.1. Përdorimi i Fjalëkalimit

[URPU_01] Përdorimi i Fjalëkalimit

Për punonjësit e IdentiTek, praktikat më të mira të sigurisë përcaktohen në dokumentin e politikës së llogarisë së përdoruesit të IdentiTek. Fjalëkalimet përputhen me rregullat e shkruara nga Shoqëria dhe kanë karakteristikat e mëposhtme:

- Kohëzgjatja maksimale
- Madhësia minimale

- Një nivel minimal i kompleksitetit (katër lloje të karaktereve) që kufizon rrezikun e gjetjes së fjalëkalimit (guessing password) (kombinim i shkronjave (shkronja kapitale/vogla), numrave dhe karaktereve speciale, ndalohet përdorimi i termave të lehtësisht të gjetshme…).

Fjalëkalimet duhet të mbrohen!

9.4. Politika për Përdorimin e Shërbimeve në Rrjet

9.4.1. Politika për Përdorimin e Shërbimeve në Rrjet

[NET_07] Kontrolli logjik i aksesit në pajisjet e rrjetit

Fjalëkalimet e paracaktuara ("default") të përdorura nga prodhuesit brenda pajisjeve ndryshohen sistematikisht. Llogaritë nominative dhe monitoruese të administratës krijohen sistematikisht. Fjalëkalimet përputhen me kërkesat e sigurisë të përcaktuara dhe të formalizuara.

Pajisjet e rrjetit dhe të drejtat e alokuara për administratorët rishikohen dhe kontrollohen rregullisht.

[NET_08] Mbrojtja e kabllove dhe treguesve të rrjetit

Portat "plugs" e rrjetit janë të identifikuar dhe vetëm portat e përdorura janë aktive.

Skemat e kabllimit të rrjetit janë të dokumentuara dhe të përditësuara.

[NET_09] Mbrojtja e administrimit të rrjetit

Administrimi dhe monitorimi i rrjetit realizohen nga pajisje ose rrjete të dedikuara.

Aksesi në portë (fizike ose logjike) për administrimin dhe monitorimin është e kontrolluar dhe e kufizuar vetëm për pajisjet ose rrjetet e dedikuara.

[NET_10] Disponueshmëria e pajisjeve të rrjetit

Pajisjet kritike të rrjetit (si ruterët, infrastruktura kryesore) janë të dublikuara ose kanë pajisje zëvendësuese.

[WIFI_01] Përdorimi i Wi-Fi në IdentiTek

Në IdentiTek, përdorimi i Wi-Fi është i kontrolluar. Përdorimi i Wi-Fi është i ndaluar në mjediset e prodhimit.

Për mjediset jo të prodhimit, një politikë specifike përcakton kërkesat e sigurisë për infrastrukturën e Wi-Fi të lejuar.

Implementimi i çdo infrastrukture Wi-Fi duhet të miratohet nga Drejtori i Divizionit të Sistemeve të Informacionit. Fortësia e kodimit për infrastrukturën Wi-Fi duhet të jetë minimalisht me algoritmin AES256.

Duhet të jetë plotësisht i audituesheëm.

Duhet të regjistrojë të gjitha veprimet e Wi-Fi dhe rrjetit.

[WIFI_02] Përdorimi i Wi-Fi jashtë IdentiTek

Përdorimi i Wi-Fi mund të jetë i nevojshëm për stacionet e punës mobile jashtë IdentiTek. Përdoruesi është ndërgjegjësuar dhe informuar për rreziqet lidhur me këtë teknologji. Ndërfaqja e stacionit të punës mobile është e çaktivizuar nga parazgjedhje dhe aktivizohet vetëm nëse është e nevojshme.

Aksesi në rrjetin e IdentiTek është e kufizuar me kujdes për të parandaluar aksesin pa autorizim. Aksesi në të gjitha sistemet dhe pajisjet kompjuterike dhe informatike është e kufizuar në mënyrë që të lejohet vetëm nëse është i miratuar.

- Aksesi i pa autorizuar në programe ose aplikacione mund të çojë në veprime keqdashëse ose të rrezikojë infrastrukturën e IdentiTek.
- Kur qasja fizike ose logjike nuk është e kontrolluar, përdoruesit mund të gjejnë (dhe të shfrytëzojnë) rrugë aksesi të paautorizuara në sistemet dhe burimet e rrjetit. Për shembull: ata mund të lidhin një laptop në një prizë murale të papërdorur, të anashkalojnë serverin e hyrjes dhe të lidhen drejtpërdrejtë me serverin kryesor.
- Aksesi pa autorizim nga jashtë në rrjetin e IdentiTek zakonisht mund të çoj në dëme, korruptim dhe humbje të konfidencialitetit të informacionit të IdentiTek.
- Te dhënat e paplota ose të pasakta të përdoruesve në profilin e tyre të aksesit në rrjet mund të rezultojnë në lejimin e tyre për të modifikuar, fshirë, ose pasur akses në informacion konfidencial në burime të paautorizuara të rrjetit.
- Modifikimet e bëra në profilin e aksesit në rrjet pa procedurat e kontrollit të ndryshimit mund të çojnë në akses të papritshëm (dhe ndoshta aksidentale) në burime të paautorizuara të rrjetit.

9.4.2. Autentifikimi i përdoruesit për lidhjet e jashtme

[UAEC_01] Lidhjet e jashtme

Kompjuterët e lejuar në distancë autentifikohen në mënyrë të thelluar "AUTENTIFIKIM RECIPROK" (mutual-authentication). Stacioni i punës të regjistrimit/dorëzimit autentifikohet me autentifikim reciprok me pajisjen qendrore të VPN. Komunikimi është i koduar dhe përdoruesi në stacionin e punës autentifikohet në sistemin qendror të përdoruesve të IdentiTek.

[EDI_01] Shërbimet aplikative dhe formalizimi i shkëmbimeve

Shërbimet aplikative dhe shkëmbimet për palët e treta si shërbime të jashtme të palëve të treta përcaktohen brenda projekteve duke përfshirë një analizë të rrezikut që lejon:

- Identifikimin e lidhjeve të nevojshme dhe rrjedhën e të dhënave në nivel funksional ose teknik.
- Përcaktimin e nevojave të tyre për sigurinë (konfidencialitet, integritet, disponueshmëri).
- Vlerësimin e rrezikut dhe rreziqet e hasura.
- Përzgjedhjen e kontrollit së sigurisë që lejojnë zvogëlimin e këtyre rreziqeve në një nivel të pranueshëm.

[EDI_02] Autorizimi i aksesit

Lejimi i aksesit të një partneri kërkon nënshkrimin e një marrëveshje kontraktuale mes kësaj pale të tretë dhe IdentiTek. Kjo është e njëjta procedurë për çdo akses me shërbimet e palës së tretë të jashtme. Këto marrëveshje kontraktuale përfshijnë aspektin e sigurisë dhe përfshihen në kontratë.

[EDI_03] Kontrolli i aksesit dhe mbrojtja e shkëmbimit të informacionit

Partneri - sistemi, aplikacioni ose përdoruesi - është gjithmonë i identifikuar dhe autentifikuar. Është i detyrueshëm përdorimi i protokolleve të sigurt (SSL, SSH) ose lidhjeve që garantojnë identitetin e partnerit (Leased Line, VPN).

Kontrolle të veçanta të sigurisë mund të kërkohen në varësi të nivelit të sensivitetit të dhënave të shkëmbyera. Preferohen metodat kriptografike (kodimi, nënshkrimi, ...).

Lidhjet e krijuara dhe shkëmbimet e informacionit janë të audituara, të regjistruara (logged) dhe të audituesheme (tracebility) sipas nevojave të biznesit dhe rregullores.

9.4.3. Identifikimi i pajisjeve në rrjete

[EQIN_01] Identifikimi i pajisjes

Çdo server në rrjetin e brendshëm të IdentiTek (LAN) është i identifikuar me një adresë IP fikse (Static IP).

9.4.4. Mbrojtja e portës të diagnostikimit dhe konfigurimit në distancë

[RDCPP_01] Mbrojtja e administrimit të rrjetit

Aksesi i portave (fizike ose logjike) për administrim dhe monitorim është i kontrolluar dhe i kufizuar në pajisje ose rrjete të dedikuara.

9.4.5. Kontrolli i lidhjes në rrjet

[NECC_01] Kontrolli i Përdorimi të rrjetit kompjuterik të IdentiTek

Përdorimi i autorizuar i rrjetit kompjuterik të IdentiTek shpjegohet tek Politika e Llogarive të përdoruesve. Kjo politikë aplikohet tek të gjithë punonjësit që kanë akses në çdo burim informacioni të IdentiTek.

9.4.6. Kontrolli i rrugëtimit (routing) të rrjetit

[NERC_01] Harta e adresave (address mapping)

Adresat IP që nuk janë të rrugëtueshme (non routable) dhe mekanizmi i përkthimit të adresave (NAT-Network Address Translation) përdoren për të mbajtur konfidencialitetin e skemës së adresimit të brendshëm. Plani i adresave IP është i përcaktuar dhe i përditësuar nga ekipi i Departamentit të Teknologjisë dhe Informacionit.

9.5. Kontrolli i hyrjes në sistemin operativ

9.5.1. Procedurat e sigurta të hyrjes

[SLOP_01] Identifikimi i sigurt

Aksesi në sistemet e IdentiTek-ut realizohen përmes një procesi të sigurt të hyrjes që përfshin:

- Njoftim të përgjithshëm që paralajmëron se sistemi është vetëm për përdorues të autorizuar.
- Tregon datën dhe kohën e hyrjes të mëparshme të suksesshme.
- Autentifikon përdoruesit vetëm pasi të gjitha të dhënat janë të dorëzuara dhe nuk tregon cilat të dhëna janë të pasakta në një tentativë të pasuksesshme.

9.5.2. Identifikimi dhe autentifikimi përdoruesit

[UIAA_01] Identifikimi dhe autentifikimi

Përdoruesit e sistemit janë të identifikuar individualisht me një llogari unike. Secilës llogari i është asociuar një fjalëkalim në përputhje me kërkesat e Politikës së Fjalëkalimeve të Shoqërisë.

9.5.3. Sistemi i menaxhimit të fjalëkalimeve

[PAMS_01] Menaxhimi i fjalëkalimit

Kontrollet e sigurisë mundësojnë sigurinë e konfidencialitetit të kodeve konfidenciale që transmetohen në rrjet (përdorimi i protokolleve të sigurisë, administrim i izoluar i rrjetit).
Kontrollet e sigurisë mundësojnë sigurinë e disponueshmërisë së fjalëkalimeve të llogarive të privilegjuara (vendosja brenda një zarfi (tamper proof) dhe ruajtja në një vend të sigurt).

9.5.4. Koha e mbylljes së sesionit

[SETO_01] Koha e mbylljes së sesionit

Ekzistojnë kontrolle sigurie për të kufizuar lidhjen e një terminali jo aktiv. Pas skadimit të kohës së konfiguruar, sesioni skadon dhe përdoruesi shkëputet. Përdoruesit i kërkohet të autentifikohet përsëri për të punuar me aplikacionin ose sistemin.

9.5.5. Kufizimi i kohës së lidhjes

[LICT_01] Koha e kufizuar e lidhjes

Përqasja në sistemin qendror të IdentiTek është i kufizuar gjatë orareve normale të punës.

9.6. Kontrolli i aksesit të aplikacionit dhe informacionit

9.6.1. Kufizimi i aksesit në informacion

[APIAC_01] Menaxhimi i të drejtave për të hyrë në aplikacione

Të drejtat e përqasjes për aplikacionet e biznesit (ndarja, përditësimi dhe heqja e të drejtave të përqasjes) bazohen në rregullat dhe procedurat e implementuara si menaxhimi i krijim/modifikim të përdoruesit dhe të drejtat e përqasjes. Të drejtat në sisteme/aplikacione janë të rishikuara rregullisht.

[APIAC_02] Kontrolli i aksesit në aplikacionin e biznesit

Përqasja në aplikacione është i kontrolluar. Ky kontroll bazohet në mekanizmat e implementuar për identifikimin dhe autentifikimin e përdoruesit, dhe të drejtat e trashëguara nga profili i tyre dhe bazuar në kontekstin e përdorimit. Këta mekanizma gjithashtu përcaktojnë përqasjen në funksionet dhe të dhënat e ndryshme brenda aplikacionit. Përqasja e alokuar e një përdoruesi është rreptësisht personale.

[APIAC_03] Aplikacionet e biznesit përdorin kontrollin dhe ndjekjen

Përdorimi i funksioneve aplikative regjistrohet dhe auditohet (bazuar në sensitivitetin e tyre dhe në të dhënat e aksesuara). Regjistrat e gjurmimit “logs” aplikative analizohen rregullisht për të zbuluar gabimet në përdorim, dështimet dhe përdorimet e paligjshme.

9.6.2. Izolimi sensitiv i sistemit

[SSIS_01] Izolimi i sistemit

Rrjetet lokale janë ndarë në VLAN (Virtual Lans) për të siguruar izolimin e sistemeve sensitive dhe për të mundësuar kufizimin (containment) në rast të një incidenti. Rrjetet e prodhimit janë të ndara nga rrjetet administrative.

10. KRIPTOGRAFIA

10.1. Kontrollet Kriptografike

10.1.1. Politika në Përdorimin e Kontrolleve Kriptografike

[CRY_01] Elementët Kriptografikë

Çelësat kriptografikë dhe certifikatat e përdorura brenda softuerit të sigurisë të ndërtuar në sistemin IdentiTek duhet të mundësohen nga infrastruktura e çelësave publikë të IdentiTek. Kushtet e përdorimit janë të përcaktuara në politikën e certifikatave të IdentiTek. Çdo përjashtim nga ky rregull duhet të aprovohet nga Drejtori i Departamentit të Sigurisë së Informacionit i IdentiTek.

[CRY_02] Sistemet Kriptografike

Sistemet kriptografike të autorizuara janë ato të identifikuara dhe të listuara në listën e mjeteve kriptografike të autorizuara. Kjo listë menaxhohet nga Departamenti i Sigurisë së Informacionit të IdentiTek.

[CRY_03] Madhësia e Çelësit dhe Algoritmet në krahasim me kohën

Çdo algoritëm që përdor çelësa asimetrikë (RSA ose DSA) me madhësi më pak se 2048 bite është i dobët dhe nuk duhet të përdoret për të siguruar një funksion kritik (autentifikim i fortë, kodimi i të dhënave sensitive ose konfidenciale etj.).

Çdo algoritëm që përdor çelësa asimetrikë (RSA ose DSA) me madhësi të barabartë me 2048 bite nuk mund të përdoret për më shumë se 3 vite.

Çdo algoritëm që përdor një çelës simetrik (DES, AES ose ekuivalent) me madhësi më pak se 128 bite është i dobët dhe nuk duhet të përdoret.

Çdo algoritëm që përdor funksionin MD5 ose SHA-1 është i dobët dhe nuk duhet të përdoret për çfarëdo lloj funksioni.

Çdo algoritëm shkëmbimi çelësi që përdor PSK, SRP dhe DSS konsiderohet i dobët dhe nuk duhet të përdoret.

Çdo komunikim VPN IPSec duhet të përdorë IKEv2 dhe jo IKEv1 për shkëmbimin e çelësave. Madhësia dhe algoritmet e rekomanduara për çiftet e çelësave të përdorura nga PKI dhe komponentët e infrastrukturës janë detajuar në një dokument të posaçëm të politikës së Kriptimit dhe Menaxhimit të Çelësave të IdentiTek.

[CRY_05] Kërkesat Minimale për TLS

Sistemet kompjuterik "server" duhet të konfigurohen për të përdorur TLS v1.2 dhe duhet të konfigurohen gjithashtu për të përdorur edhe TLS v1.3. Sistemet kompjuterik "server" nuk duhet të konfigurohen për të përdorur TLSv1.1 dhe nuk duhet të përdorin TLSv1.0, SSL 3.0 ose SSL 2.0.

TLS duhet të konfigurohet në nivel serveri minimalisht, me një certifikatë nënshkrimi RSA ose një certifikatë nënshkrimi ECDSA. Nëse sistemi kompjuterik "server" është i konfiguruar me një certifikatë nënshkrimi ECDSA, duhet të përdoret kurba P-256 ose kurba P-384 për çelësin publik në certifikatë.

10.1.2. Menaxhimi i çelësave

[CRY_04] **Menaxhimi i çelësave.** Dokumenti "Praktika e Certifikatave" shpjegon përdorimin, mbrojtjen dhe jetëgjatësinë e çelësave kriptografike përgjatë të gjithë ciklit të tyre të jetës.

11. SIGURIA FIZIKE DHE MJEDISORE

11.1. Zonat e Sigurta

11.1.1. Përkufizimi i kufijve të sigurisë fizike

[PHY_01] Përkufizimi i kufijve të sigurisë fizike

Për të evituar çdo hyrje të paautorizuar fizike, dëmtim ose ndërhyrje, brenda ambienteve dhe të dhënave të IdentiTek, është përcaktuar perimetri i sigurisë fizike në këtë mënyrë:

- Zona 1: kjo zonë është e destinuar për mirëseardhjen e publikut.
- Zona 2: kjo zonë është e rezervuar për shërbimin, e izoluar nga zona publike me hyrje të kontrolluar nga roje dhe e rezervuar për punonjësit e IdentiTek. Vizitorët nuk kanë qasje në këtë zonë pa një kartë vizitori elektronike, e cila është dorëzuar nga oficerët e sigurisë të IdentiTek dhe nga persona përgjegjës për shoqërimin e vizitorit.
- Zona 3: Kjo zonë është sensitive dhe jep qasje në zyrat e personelit të menaxhimit ose punonjësve të besuar. Këto zona janë të mbrojtura nga sistemi i kontrollit të hyrjes fizike (kartë, biometri, kod). Vizitorët nuk kanë qasje në këtë zonë pa një kartë vizitori elektronike të dorëzuar nga persona përgjegjës për shoqërimin e tyre. Vizitorët duhet të jenë gjithmonë të shoqëruar.
- Zona 4: këto zona janë të dedikuara për ambientet TI (serverë, pajisjeve) dhe rrjetit. Këto janë ambiente të dedikuara brenda ndërtesës së IdentiTek të mbrojtura nga hyrja fizike e kontrolluar. Hyrja në këtë zonë monitorohet në mënyrë të veçantë; mbajtja e kartës së aksesit është e detyrueshme dhe duhet të jetë e dukshme. Lista e personave të autorizuar për hyrjen në këto zona shqyrtohet dhe përditësohet periodikisht. Shfuqizimet realizohen në kohë reale.
- Zona 5: kjo zonë është e dedikuar mjedisit të teknologjisë së informacionit të PKI dhe ndodhet brenda dhomës së serverëve të IT-së. Hyrja në këtë zonë monitorohet në mënyrë të veçantë; mbajtja e kartës së aksesit është e detyrueshme dhe duhet të jetë e dukshme.. Lista e personave të autorizuar për hyrjen në këto zona shqyrtohet dhe përditësohet periodikisht. Revokimet realizohen në kohë reale.

11.1.2. Kontrollet e Hyrjes Fizike

[PHY_02] Zbatimi i Kontrolleve të Hyrjes

Një sistem aksesi kontrolli me dy faktorë autentifikimi (karte aksesi, kod ose shenje biometrike) është i vendosur në zonat 2, 3, 4 dhe 5. Aksesi monitorohen dhe të dhënat e aksesit ruhen.

[PHY_03] Menaxhimi i të Drejtave të Hyrjes Fizike

Kërkesat për autorizim të hyrjes në zonën 4 janë të aprovuara nga Drejtori i Divizionit të Sistemeve të Informacionit në IdentiTek, dhe Menaxherin e Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes. Kërkesat për autorizim të hyrjes në zonën 5 janë të aprovuara nga Drejtori i Divizionit të Sistemeve të Informacionit në IdentiTek. Hyrjet jepen bazuar në një kërkesë formale dhe të motivuar lidhur me nevojën për informacion. Kërkesat për autorizim të hyrjes ruhen në arkiv.

[PHY_04] Kontrolli i Autorizimit të Hyrjes dhe Pasqyrimi i saj

Çdo Menaxher i zonës mbart në përgjegjësinë e tij një listë të personave që kanë autorizim për hyrjen në zonë. Kjo listë e hyrjeve shqyrtohet dy herë në vit.

11.1.3. Mbrojtja e Zyrave, Dhomave dhe Pajisjeve

[SECO_04] Mbrojtja e Zyrave, Dhomave dhe Pajisjeve

Të gjitha zyrat, dhomat dhe pajisjet e sigurta janë të mbyllura dhe hyrja në to është e kontrolluar. Të gjitha dritaret janë të monitoruara nga një sistem zbulimi për ndërhyrje të paautorizuar.

Në të gjithë godinën e IdentiTek, ka kamera për të monitoruar jashtë dhe brenda objektit.

Të gjitha informacionet jo-elektronike, kryesisht bazuar në letër, si PP (Personal Papers); ERP (Electronic Records and Procedures) dhe letërnjoftimet elektronike, dokumentet e zbrazëta, arkivi i dokumenteve, deklarata financiare etj., ruhen në një Zonë të Sigurt të mbrojtur nga kontrolli i hyrjes. Të dhënat e mbrojtura dhe të kufizuara ruhen në mënyrë të sigurtë përmes dollapëve të mbyllur dhe/ose kasafortave të mbyllura.

Të gjitha pajisjet si kompjuterët dhe/ose stacionet e punës që trajtojnë të dhëna sensitive vendosen në vende të sigurta për të evituar rrezikun që të dhënat të jenë të ekspozuara ose të shihen nga persona të paautorizuar.

11.1.4. Mbrojtja Nga Kërcënime të Jashtme dhe Mjedisore

[PHY_05] Mbrojtja nga zjarri

Është përcaktuar një set procedurash reagimi kundër katastrofave si zjarri. Për këtë qëllim, pajisjet e shuarjes së zjarrit janë të instaluar brenda ndërtesës së IdentiTek, daljet e emergjencës janë të shënuara dhe planet e evakuimit janë të shfaqura. Pajisjet e shuarjes së zjarrit kontrollohen dhe vendi ndodhet në monitorim të vazhdueshëm.

[PHY_06] Trajnimi kundër zjarrit

Trajnimi dhe ndërgjegjësimi i punonjësve për të luftuar kundër këtyre katastrofave realizohen përmes ushtrimeve simuluese, të ndjekura nga analiza e reagimeve dhe sjelljes për të organizuar, nëse është e nevojshme, sesione shtesë trajnimi.

[PHY_07] Zbulimi i zjarrit

Për të parandaluar dhe zbuluar ngjarjet si zjarri, është instaluar një sistem zbulimi i zjarrit në ambientet e IdentiTek.

11.1.5. Puna në Zonat e Sigurta

[ËSA_01] Ndërgjegjësimi i personelit për sigurinë

Të gjithë punonjësit e IdentiTek janë të ndërgjegjshëm për rutinën/praktikën e përditshme të kontrolleve të sigurisë, si mbajtja dhe përdorimi i një karte për hyrjen në ndërtesë.

[ËSA_02] Pajisjet e ndaluara në zonat e sigurta

Pajisjet e regjistrimit fotografik, video, audio ose të tjera, si kamerat në pajisjet mobile, nuk lejohen në perimetrin e sigurisë, përveç nëse është autorizuar nga drejtuesit.

[ËSA_03] Zonat e sigurta të lëna të zbrazëta

I gjithë personeli duhet të sigurohet që të gjitha zyrat/dhomat dhe dritaret janë të siguruara dhe të mbyllura si duhet kur përfundojnë punën.

[ËSA_04] Puna pa mbikëqyrje në zonat e sigurta

Personeli i mirëmbajtjes që hyn në zonën e kufizuar duhet të regjistrohet për hyrjen dhe daljen, dhe të shoqërohet nga personeli i përgjegjës dhe të mbajë kartën e vizitorit.

11.1.6. Zona e Hyrjes Publike, Dorëzimit dhe Ngarkimit

[PBA_01] Punimi pa mbikëqyrje në zonat e sigurta

Hyrja në një zonë dorëzimi dhe ngarkimi nga jashtë ndërtesës është e kufizuar për personelin e identifikuar dhe të autorizuar. Materialet hyrëse janë të inspektuara dhe të regjistruara.

11.2. Siguria e Pajisjeve

11.2.1. Vendndodhja dhe Mbrojtja e Pajisjeve

[EQS_01] Mbrojtja fizike dhe mjedisore e pajisjeve

Çdo pajisje është e identifikuar me një referencë të etiketuar dhe është e inventarizuar. Ekziston një inventar pajisjesh dhe përmban të gjitha pajisjet, vendndodhjen dhe karakteristikat e tyre.

[EQS_02] Identifikimi i pajisjeve

Çdo pajisje është e identifikuar me një referencë dhe është e inventarizuar. Ekziston një inventar pajisjesh dhe përmban të gjitha pajisjet, vendndodhjen dhe karakteristikat e tyre.

11.2.2. Shërbimet Mbështetëse

[SUUT_01] Përshtatshmëria e pajisjeve ndihmëse

Të gjitha vendndodhjet e IdentiTek kanë pajisje ndihmëse të nevojshme për të operuar pajisjet kompjuterike dhe për sigurinë e tyre: ngrohje/ajrim, kondicionim i ajrit, furnizim me ujë, pajisje kundër zjarrit (shuarës zjarri CO2, shuarës zjarri me pluhur të thatë, sistemi i zjarrit), furnizim me energji elektrike (UPS, transformator, gjenerator), mjetet e telekomunikacionit (linja,...).

Shpërndarja e realizuar e pajisjeve ndihmëse lejon sigurimin e operimit të duhur të pajisjeve kompjuterike dhe rrjetit në ambientet e IdentiTek, si dhe sigurinë e tyre.

[SUUT_02] "Redundanca" e pajisjeve ndihmëse

Pajisjet ndihmëse në ambientet e IdentiTek kanë një nivel të mjaftueshëm "redundancy" për të siguruar operimin e duhur të infrastrukturës dhe pajisjeve kompjuterike në përputhje me planin e vazhdimësisë së biznesit.

[SUUT_03] Mirëmbajtja e pajisjeve ndihmëse

Pajisjet ndihmëse janë të mbuluara nga kontratat e mirëmbajtjes dhe nëse është e nevojshme nga kontratat e shërbimit që lejojnë disponueshmërinë e shërbimit të dhënë nga këto pajisje.

Nën-kontraktorët të cilët janë përgjegjës për këto kontrata firmosin një kontratë konfidencialiteti.

11.2.3. Siguria e Kabllimit

[SUUT_04] Mbrojtja e kabllimit

Dhoma e "serverave" ka dysheme teknologjike të përshtatshme dhe kanale që lejojnë një kalim të sigurt të kabllove të ndryshëm.

Prizat e rrjetit janë të identifikuara dhe lidhen vetëm me portat e përdorura. Hyrja në panelet e lidhjeve është e kontrolluar. Hyrja në linjën kryesore të telekomunikacionit është e kontrolluar dhe e mbrojtur. Kabllot e infrastrukturës së rrjetit janë të mbrojtura nga rreziqet e ndërhyrjes dhe dëmtimit.

Skemat e kabllimit të rrjetit janë të dokumentuara dhe të përditësuara.

11.2.4. Mirëmbajtja e Pajisjeve

[EQS_03] Mirëmbajtja e pajisjeve

Pajisjet mirëmbahen vetëm nga personeli i mirëmbajtjes i autorizuar nga IdentiTek.

11.2.5. Siguria e Pajisjeve Jashtë Objektit

[EQS_04] Dalja e pajisjeve

Rregullat dhe procedurat për daljen e një pajisjeje janë formalizuar dhe të dokumentuara. Ato marrin në konsideratë sensitivitetin e të dhënave në pajisje dhe formalizojnë kontrollin e ndjekjes jashtë objektit për të siguruar mbrojtjen e aseteve të IdentiTek. Çdo pajisje regjistrohet dhe autorizohet para daljes.

Stacionet e regjistrimit/shpërndarjes ndodhen jashtë zyrave qendrore. Vendet ku ndodhen stacionet e punës janë në përgjegjësi të Ministrisë së Brendshme.

11.2.6. Ripërdorimi dhe Shkatërrimi i Sigurt i Pajisjeve

[SDRE_01] Ripërdorimi i pajisjeve

Para riciklimit të çdo pajisjeje, informacioni sensitiv fshihet në mënyrë që të jetë e pamundur të rikthehet. Fshirja e të dhënave sensitive dhe zonave që kanë mbajtur të dhëna sensitive realizohet me mjete të mundësuara nga Departamenti i Teknologjisë dhe Informacionit.

[SDRE_02] Shkatërrimi i Sigurt i pajisjeve

Procedurat për heqjen e aseteve sensitive janë formalizuar dhe komunikohen te të gjithë punonjësit e IdentiTek. Shkatërrimi i mediave elektronikë bëhet në mënyrë të sigurt përmes grirjes. Mediat për ruajtjen e të dhënave (disqet, shiritat magnetike...), kartat dhe komponentët elektronikë sensitivë goditen me çekiç ose këputen.

11.2.7. Heqja e mjeteve në pronësi

[EQS_05] Heqja e mjeteve në pronësi

Para se të fillojë riciklimi ose heqja, çdo pajisje që përmban media të ruajtjes kontrollohet, fshihet dhe çdo software i licencuar ç'instalohet. Fshirja e të dhënave sensitive realizohet me mjete të siguruara nga Departamenti i Teknologjisë dhe Informacionit.

11.2.8. Pajisje të pa Mbikëqyrura të Përdoruesit

[WSTAT_01] Rikujtesa e rregullave për mbrojtjen e stacioneve të punës

Rregullat kryesore dhe dispozitat lidhur me sigurinë dhe përdorimin e stacioneve të punës përmendet në politikën e llogarisë së përdoruesit për mirëpërdorimin e sistemit të informacionit dhe janë në dispozicion për të gjithë. Rregullat ri-kujtohen gjatë sesioneve periodike të ndërgjegjësimit të përdoruesve.

[WSTAT_02] Pajisje të pa Mbikëqyrura

Çdo përdorues duhet të mbyllë stacionin e punës kur nuk është në vendin e tij, pasi çdo sesion i lënë hapur mund të përdoret nga persona të panjohur dhe përdoruesi i autentifikuar mbahet përgjegjës për çdo pasojë.

11.2.9. Politika e Tryezës dhe Ekranit të Pastër

[CDCSP_01] Politika e Tryezës dhe Ekranit të Pastër

Çdo përdorues duhet të pastrojë tryezën e tij në mënyrë që të ruajë të dhënat sensitive (dokumente, letra, media e lëvizshme,..) në vendin e ruajtjes të përshtatshëm si kasaforta, dollapë, dhomë e mbrojtur.

12. SIGURIA OPERACIONALE

12.1. Procedurat dhe Përgjegjësitë Operative

12.1.1. Procedurat operative të dokumentuara

[DOCO_01] Dokumentacioni i procedurës operative

Procedurat operacionale të sistemeve të TI janë të dokumentuara.

Ky dokument shpjegon udhëzimet që duhen ndjekur për çdo detyrë të lidhur me administrimin, operimin, monitorimin dhe mirëmbajtjen e sistemeve të informacionit. Ai mbahet i përditësuar, aktualizohet nëse është e nevojshme, dhe rishikohet të paktën një herë në vit.

Vetëm personat që kanë nevojë për informacion mund të kenë akses në këtë dokumentacion.

[DOCO_02] Administrimi dhe monitorimi

Administrata dhe monitorimi i serverëve realizohen nga personeli i autorizuar nga mjediset e mbrojtura (ambientet, VLAN, konsole të monitorimit).

Fluksi i rrjetit (network flow) i administrimit dhe monitorimit është i mbrojtur në aspektin e konfidencialitetit.

Veprimet e administrimit dhe monitorimit janë të audituara dhe rishikohen periodikisht.

12.1.2. Menaxhimi i ndryshimeve

[CHM_01] Menaxhimi i ndryshimeve dhe konfigurimeve

Konfigurimet e sistemeve të TI dhe ndryshimet në këto sisteme janë të menaxhuara dhe kontrolluara me kujdes duke marrë në konsideratë temat e mëposhtme:

- Një procedurë përshkruan kushtet e zbatimit të çdo ndryshimi
- Ndikimet e ndryshimeve janë të vlerësuara dhe ndryshimet janë të testuara. Ndryshimet e mëdha janë të planifikuara. Duhet të përcaktohet një procedurë për kthim mbrapa “roll back”.
- Konfigurimet e TI janë të dokumentuara. Të gjitha ndryshimet janë të regjistruara.

12.1.3. Menaxhimi i Kapaciteteve

[CAMA_01] Disponueshmëria sensitive e serverit

Kontrolluesit e domain-it, serveri i bazës së të dhënave të qytetarëve, serverët e MBSS, serverët e MorphoCivis dhe serverët e MorphoPerso janë “redundant”.

[CAMA_02] Monitorimi i kapacitetit të burimeve

Përdorimi i burimeve të IdentiTek është i monitoruar në mënyrë të vazhdueshme në mënyrë që të parandalohet çdo bllokim i mundshëm.

12.1.4. Ndarja e Detyrave

[SEGOD_01] Ndarja e Detyrave

Për të kufizuar riskun e gabimeve ose përdorimit të gabuar, është vendosur një ndarje e detyrave dhe përgjegjësive:

- Në nivelin funksional, midis
  - Administratorëve të Sistemit TI dhe Rrjetit
  - Administratorëve të Bazës së të Dhënave IT
  - Administratorëve të PKI dhe HSM
  - Administratorëve të HSM dhe Administratorëve të Regjistrimit të Logeve
  - Administratorëve të Sistemit dhe Administratorëve të Aplikacionit
  - Administratorëve të TI dhe Kontrollit të Aksesit së Kamerave dhe Kontrollit të Hyrjes (të bërë nga Departamenti i Sigurisë Logjistikës dhe Mirëmbajtjes)
  - Operatorit LRA (Local Registration Authority) dhe Administratorëve PKI
  - Audituesit dhe Administratorëve të Sistemit ose Rrjetit ose Administratorëve të PKI ose Administratorëve të HSM.
- Në nivelin e sistemit, midis
  - Personelit përgjegjës për operimin e infrastrukturës së mbështetjes së TI (p.sh., operatorët, administratorët e nivelit të parë (IT support)
  - Personelit përgjegjës për kontrollin e përdorimit të komponentëve të ndryshëm të infrastrukturës dhe përgjegjës për politikat e sigurisë në to për shembull, administratorët e nivelit 2 të IT)
  - Dhe personelit përgjegjës për auditimin.
- Në nivelin e llogarive aplikative ose të biznesit, midis
  - Personave përgjegjës për miratimin e të drejtave të aksesit aplikativ ose të biznesit
  - Personave që përdorin llogaritë aplikative ose të biznesit
  - Personave përgjegjës për caktimin e të drejtave
  - Dhe personave përgjegjës për auditimin e llogarive.

12.1.5. Ndarja e mjediseve të zhvillimit, testimit dhe operimit

[SEPE_01)Ndarja e mjedisit

Mjetet dhe mjediset e ndryshme për aplikacione sensitive (zhvillim, testim, dhe operim) janë të ndara.

Rregullat për kalimin nga një mjedis në tjetrin janë të formalizuara dhe të dokumentuara.

Të dhënat operative duhet tu hiqen "sanitized" informacionet sensitive nëse është e nevojshme për përdorim në zhvillim ose testim.

12.2. Mbrojtja kundër qëllimeve keqdashëse

12.2.1. Mbrojtje kundër kodeve me qëllim keqdashës ose malware

[VIR_01] Politika e Antivirus dhe Malware

IdentiTek ka një politikë antivirusi që mundëson mbrojtjen e sistemeve kundër viruseve, "worms" dhe menaxhon dhe zvogëlon sulmet e viruseve.

[VIR_02] Disponueshmëria e antivirusit dhe përdorimi i përditshëm

Departamenti i Teknologjisë dhe Informacionit siguron rregullisht që çdo pajisje e prekur të ketë një antivirus aktiv dhe të përditësuar dhe kontrolli i antivirusit është i planifikuar në frekuencë javore për skanime të plota.

Antivirusi i instaluar në stacionin e punës kryen një skanim javor të të gjithë diskut të vendosur në makinë për të siguruar që nuk ka viruse në stacionin e punës.

[VIR_03] Zbulimi dhe trajtimi i virusit

Të gjithë viruset e zbuluar shkaktojnë automatikisht një alarm për ekipin përkatës të Departamentit të Teknologjisë dhe Informacionit, përmes sinjalizimeve vizuale në ekranet e monitorimit të dedikuar dhe përmes regjistrimit në "logs". Këto regjistra shqyrtohen çdo ditë.

[VIR_04] Bllokimi i viruseve/përditësimi i antivirusit

Për laptopët, një terminal i dekontaminimit (një rrjet i vogël me një server përditësimi antivirus) lejon përdoruesit të kthehen në zyrat qendrore të IdentiTek për të kryer një përditësim dhe një skanim të laptopëve të tyre për të zvogëluar riskun për shoqërinë IdentiTek.

12.3. Back-Up

12.3.1. Informacioni Back-Up

[BACK_01] Politika Backup

IdentiTek ka një politikë të formalizuar për sigurinë e kopjeve rezervë. Kjo politikë merr në konsideratë nevojat për siguri të të dhënave të biznesit dhe të dhënave të brendshme dhe merr në konsideratë kohën e nevojshme për t'i rikthyer ato.

Politika e kopjeve rezervë është, të paktën, e rishikuar një herë në vit. Ajo përditësohet në çdo evolucion të Teknologjisë së Informacionit.

[BACK_02] Politika e Rikthimit

Politikat e Rikthimit janë të formalizuara. Testimi i rikthimit kryhet periodikisht.

[BACK_03] Menaxhimi dhe siguria e mediave rezervë

Mediat rezervë mbahen në ambiente të sigurta ose në dollapë të kyçur të përshtatur me nivelin e tyre të sensitivitetit (ekuivalent me nivelin e të dhënave rezervë). Këto ambiente janë të vendosura mjaft larg nga sistemet rezervë për të shmangur shkatërrimin e tyre ose kopjeve rezervë. Dollapët e kyçura të përdorura për ruajtjen e mediave rezervë janë të mbrojtura nga zjarri.

Hyrja në ambiente ose në dollapët e mbyllur janë të autorizuara për një numër të kufizuar personash.

[BACK_04] Ruajtja jashtë e mediave rezervë (offsite)

IdentiTek duhet të ketë një depo jashtë qytetit të Tiranës në një distancë minimalisht prej 60 kilometrash. Kushtet mjedisore për ruajtjen e mediave të rezervës monitorohen nga IdentiTek.

12.4. Monitorimi

12.4.1. Regjistrimi (Logging) i Auditimit

[MONI_01] Regjistrimi i auditimit të ngjarjeve

Mekanizmat e auditimit sigurojnë regjistrimin në dosjet e auditimit të ngjarjeve kryesore të lidhura me sigurinë.
Ky regjistrim merr parasysh ngjarjet e mëposhtme:

- Anomali që mund të zbulonin incidente të sigurisë;
- Probleme të sigurisë: zbulimi i viruseve, tentativat për ndërhyrje, gabimet në lidhje (connection errors);
- Aktiviteti i personave të përgjegjshëm për administrimin e sistemeve të informacionit: konfigurimi dhe vendosja e sistemeve, menaxhimi i të drejtave të hyrjes dhe privilegjeve;
- Ngjarjet lidhur me përdorimin e rrjeteve: hyrja në rrjet, faqet e vizituara, lidhjet mobile;
- Aktiviteti i përdoruesit të sistemit: lidhjet dhe shkëputjet (log off), hyrja dhe përdorimi i burimeve të rëndësishme të sistemit të informacionit.

Është përgjegjësi e Drejtorit të Divizionit të Sistemeve të Informacionit të IdentiTek, në bashkëpunim me Menaxherin e Sigurisë së Informacionit dhe Administratorit të IdentiTek, të sigurojë që informacioni i regjistruar përputhet me kërkesat rregullatore dhe ligjore për përmbajtjen e gjurmimit dhe për informacionin privat të përdoruesve.

Regjistrat e auditimit janë asete sensitive të kopjuara "back-up" dhe të mbrojtura. Ato ruhen gjatë një kohe të mjaftueshme për t'iu përgjigjur nevojave operative dhe për të përmbushur kërkesat ligjore, kontraktuale ose rregullatore.

Regjistrat mund të rishikohen për të zbuluar dhe hetuar incidente të sigurisë. Ngjarjet që tregojnë një problem të mundshëm të sigurisë analizohen.

12.4.2. Monitorimi i Përdorimit të Sistemit

[MONI_02] Monitorimi i vazhdueshëm i sistemeve dhe rrjeteve

Departamenti i Teknologjisë dhe Informacionit siguron monitorimin e vazhdueshëm të sistemeve dhe rrjeteve nën përgjegjësinë e tij.

Ky monitorim përfshin veçanërisht:

- Kontrollin e operimit të saktë të sistemit të informacionit
- Kontrollin e ngarkesës së sistemeve dhe rrjeteve dhe disponueshmërinë e tyre
- Përdorimin e sistemeve dhe rrjeteve të informacionit
- Aktivitetin e personave të përgjegjshëm për administrimin e sistemit të informacionit: konfigurimin dhe vendosjen e sistemeve, menaxhimin e të drejtave të qasjes dhe të privilegjeve.

Ky monitorim bazohet në mjete të dedikuara dhe të mbrojtura, eventualisht të përbashkëta me ato të përdorura për administrimin dhe operimin e sistemeve dhe rrjeteve.

12.4.3. Mbrojtja e informacionit të regjistrit

[MONI_03] Mbrojtja e pajisjeve të regjistrimit dhe informacionit të regjistruar

Është e domosdoshme të sigurohet që pajisjet e regjistrimit dhe të dhënat e regjistrimit të arkivuara dhe të audituara të mbrohen kundër ndryshimeve të paautorizuara.

12.4.4. Regjistrat (Logs) e Administratorit dhe Operatorit

[MONI_04] Regjistrat e Administratorit dhe Operatorit

Aktivitetet e personave përgjegjës për administrimin dhe funksionimin e sistemeve të informacionit dhe vendosjen e të drejtave të aksesit dhe menaxhimit të privilegjeve në sistem duhet të regjistrohen.

12.4.5. Fault Logging

[MONI_05] Regjistrimi i gabimeve

Regjistrimi i gabimeve mund të zbuloj anomali apo incidente sigurie.

12.4.6. Sinkronizimi i orës

[MONI_06] Sinkronizimi i orës

Është e nevojshme të sinkronizohen orët e sistemeve të ndryshme nga një burim kohor i përbashkët për të garantuar përputhjen e kohës së shënuar me datën dhe orën reale. Ky sinkronizim i sistemeve të ndryshme kërkohet për të marrë raporte auditimi të sakta që përdoren në hetimet ose si prova në raste gjyqësore.

12.5. Kontrolli i Softuerit Operativ

12.5.1. Instalimi i Softuerit në sistemet operative

[COPS_01] Dokumentimi i procedurave operative

Procedurat operative janë të dokumentuara dhe marrin parasysh kontrollet e sigurisë, teknike apo organizative.

[COPS_02] Menaxhimi dhe kontrolli i zbatimit operativ

Operacionet e mirëmbajtjes janë të dokumentuara (perimetri, veprime) dhe janë të planifikuara në bashkëpunim me përdoruesit.

Janë vendosur kontrolle (për shembull, ”non regression-testing”) për të verifikuar se operacioni i mirëmbajtjes të kryer nuk ka ndryshuar sistemin operativ.

Kontrolle të vendosur për të garantuar një procedurë rikthimi në rast dështimi ose ndryshimi të të dhënave pas operacionit të realizuar të mirëmbajtjes.

Akseset e nevojshme për mirëmbajtësit jepen gjatë kohës së ndërhyrjes së planifikuar për mirëmbajtje dhe mbyllen menjëherë pas përfundimit të saj.

Një prani e përhershme me mirëmbajtësit mbahet gjatë operimit të mirëmbajtjes.

Operacionet e mirëmbajtjes të kryera regjistrohen dhe auditohen.

[COPS_03] Mirëmbajtja në distancë

Shërbimet e mirëmbajtjes në distancë rregullohen sistematikisht me marrëveshje kontraktuale që përcaktojnë kushtet në të cilat kryhen operacionet e mirëmbajtjes në distancë.

Akseset e mirëmbajtjes në distancë (llogaritë e dedikuara, akseset në rrjet) mbyllen jashtë dritareve të mirëmbajtjes në distancë. Llogaritë dhe akseset në rrjet hapen me kërkesë të mirëmbajtjes në distancë në koordinim me stafin e prodhimit IdentiTek dhe mbyllen në fund të të gjitha operacioneve të mirëmbajtjes në distancë.

Është e nevojshme të sigurohet, nëpërmjet kushteve të përdorimit, që mirëmbajtësit në distancë të informojnë sistematikisht ekipin e prodhimit në fund të çdo operacioni mirëmbajtjeje për t'i mundësuar mbylljen e aksesit.

Operacionet e mirëmbajtjes në distancë regjistrohen dhe auditohen. Ekziston një kontroll sistematik pas operacioneve të mirëmbajtjes.

12.6. Menaxhimi i Vulnerabiliteteve Teknike të Rrezikshme

12.6.1. Kontrolli i Vulnerabiliteteve Teknike të Rrezikshme

Ky proces lejon që të informohemi në kohën e duhur për çdo dobësi teknike të lidhur me sistemet e informacionit në prodhim, për të vlerësuar ekspozimin e sistemeve të TI ndaj këtyre dobësive dhe për të zbatuar veprimet e duhura për trajtimin e rrezikut të lidhur me ato.

[VULN_01] Shërbimi njoftues dhe vlerësues i dobësive

Një shërbim njoftimi për sigurinë, mundëson marrjen e informacionit në kohën e dëshiruar lidhur me cënimet e identifikuara dhe patch-et e publikuara nga redaktorët e softuerëve ose nga faqet e autorizuara (p.sh. CERT, CISA ose Nist - NVD).
Niveli kritik i çdo cënimi (p.sh. ndikimi që rezulton nga shfrytëzimi i tyre) dhe i çdo patch (që do të thotë problem i trajtuar) vlerësohet, si dhe veprimet që duhet të kryhen. Ky vlerësim përfshin kriteret e urgjencës në mënyrë të paracaktuar, nivelet janë si vijon:

- Korrigjimi i cënimeve të sigurisë në serverët kritikë: I menjëhershëm (1 javë). Serverët kritikë janë serverët e ekspozuar në DMZ.
- Patch-et e tjera të sigurisë: nisin një analizë të cënimeve për të vlerësuar nivelin e menjëhershëm nga niveli i ndikimit dhe probabiliteti i cenueshmërisë.

[VULN_02] Menaxhimi i përditësimeve dhe patch-eve

Disa kontrolle mundësojnë sigurimin e autenticitetit të përditësimeve dhe patch-ve të ngarkuara ose të marra. Veçanërisht, ato që lidhen me produkte komerciale të softuerit merren vetëm nga faqet e redaktorëve të softuerit ose nga një burim i besuar (p.sh. CERT). Integriteti i tyre kontrollohet gjithmonë.

Për sistemet dhe aplikacionet kritike, përditësimet dhe patch-et testohen dhe validohen paraprakisht para instalimit të tyre (p.sh. instalimi në firewall të brendshme ose serverët e besuar) ose para

implementimit të tyre në mjediset e testimit (PPE – Pre Production Environment) të mjediseve të prodhimit. Këto testime përfshijnë teste të kompatibilitetit me mjedisin ekzistues dhe teste të jo-regresionit (non-regression testing).

Përditësimet dhe patch-et aplikohen në një periudhë kohore bazuar në nivelin e tyre kritik, dhe nivelin e urgjencës së tyre. Një program "patch management" përcakton rregullat e implementimit në momentet më të volitshme, veçanërisht për serverët kritikë.

[VULN_03] Kufizime gjatë instalimeve të softuereve

Në kompjuter mund të instalohet vetëm softuer i validuar dhe i autorizuar. Përdoruesit përfundimtarë nuk mund të instalojnë asnjë softuer në kompjuterët e tyre.

12.6.2. Përdorimi i "veglave" të sistemit (System Utilitiy Tools)

[UOSU_01] Përdorimi i "veglave" të sistemit

IdentiTek ka kufizuar dhe kontrollon ngushtësisht përdorimin e "tools" të sistemit. Përdoruesit e IdentiTek nuk janë administratorë të stacioneve të tyre të punës. Vetëm administratorët e Teknologjisë së Informacionit të IdentiTek mund të kenë akses në përdorimin e "veglave" të sistemit. Përdorimi i këtyre shërbimeve gjurmohet.

12.7. Konsideratat e auditimit të sistemeve të informacionit

12.7.1. Kontrollet e Auditimit të Sistemeve të Informacionit

[AUD_01] Kontrollet e auditit

Kontrollet dhe testet e auditimit realizohen periodikisht të paktën një herë në vit. IdentiTek siguron që ky periodicitet të respektohet, identifikon veçanërisht dhe jep burimet për të ekzekutuar këto kontrolle. Janë marrë masa organizative për të formalizuar procedurat, kërkesat dhe përgjegjësitë.

Këto kontrolle dhe teste auditimi kryhen nga një ekip i ndryshëm nga ekipi përgjegjës për administrimin e Teknologjisë së Informacionit.

[AUD_02] Analiza e rezultateve të auditimit

Përdorimi i këtyre rezultateve mundëson rishikimin e politikës së sigurisë së informacionit

12.7.2. Mbrojtja e Mjeteve të Auditimit të Sistemeve të Informacionit

[AUD_03] Mbrojtja e mjeteve të auditimit

Mjetet dhe shërbimet e auditimit mbahen në media të mbrojtura brenda kasafortës të Menaxherit të Departamentit të Sigurisë së IT, në mënyrë që të sigurohet që vetëm personi përgjegjës për auditimin të ketë akses.

13. SIGURIA E KOMUNIKIMIT

13.1. Menaxhimi i Sigurisë së Rrjetit

13.1.1. Kontrollet e rrjetit

[NET_01] Identifikimi i Infrastrukturës së Rrjetit

Infrastruktura e rrjetit është e listuar dhe e dokumentuar. Ka një përshkrim të përditësuar të kësaj infrastrukture, i cili përfshin:

- Një skeme të rrjetit që identifikon elementet kryesore të infrastrukturës dhe paraqet organizimin e përgjithshme të rrjetit (Service Line, LAN, qasje në internet, qasje të tjera)
- Një dokument për sigurinë e rrjetit që definon infrastrukturën e rrjetit (ndërfaqet jashtë, pajisjet e rrjetit)
- Një listë të rrjedhës së trafikut kryesor të brendshëm dhe të jashtëm
- Një përshkrim të kabllimit të brendshëm
- Një inventar të pajisjeve dhe vendndodhjen e tyre
- Një përshkrim të mjeteve të sigurisë të përdorur (filtrimi, kodimi, autentifikimi) dhe implementimin operacional të tyre në pajisjet e sigurisë të rrjetit.

Dokumentacioni i rrjetit përditësohet për çdo modifikim të rrjedhës së të dhënave “network flows” ose infrastrukturës teknike të rrjetit. Të paktën një herë në vit bëhet një rishikim.

[NET_02] Mbrojtja e dokumentacionit të rrjetit dhe të dhënave të rrjetit.

Elementët (dokumentet, dosjet) që përshkruajnë infrastrukturën e rrjetit dhe konfigurimin e saj janë informacione sensitive dhe janë të mbrojtura nga aksesi i paautorizuar nga persona që nuk kanë nevojë të dinë.

Kontrollet e sigurisë të zbatuara sigurojnë disponueshmërinë dhe integritetin e këtyre elementeve.

13.1.2. Siguria e Shërbimeve të Rrjetit

[NET_04] Kontrolli i aksesit të rrjetit

Çdo fluks hyrës ose dalës i nënshtrohet autorizimit paraprak. Kërkesa zyrtarizohet nga kërkuesi dhe vërtetohet nga menaxheri hierarkik dhe autorizohet nga Menaxheri i Departamentit të Sigurisë së Informacionit.

Aksesi në Internet është individual, i autentifikuar dhe i regjistruar.

Për aksesin e lëvizshëm (Laptopë etj.) përdoret një mekanizëm i fortë autentifikimi "strong authentication mechanism".

[NET_11] Mbrojtja e serverëve në internet

Serverët që hostojnë faqet e internetit dhe shërbimet Web të aksesueshme përmes Internetit strehohen në DMZ.

Serverët mbrohen nga aksesi nga jashtë nga pajisjet fundore të sigurisë (si p.sh. Reverse Proxies).

Testet e ndërhyrjeve (Intrusion Tests) duhet të kryhen rregullisht nga interneti - të paktën një herë në vit, në mënyrë që të vlerësohet siguria e serverëve dhe web-shërbimeve duke u siguruar që një shkelje në një shërbim web nuk ndikon në LAN-in e brendshëm.

[NET_05] Mbrojtja e rrjedhës së rrjetit

Lëvizjet ose shkëmbimet e të dhënave të klasifikuara si konfidenciale janë të koduara. Kodimi i rrjedhës përdoret për të lidhur dy segmente rrjeti të të njëjtit nivel konfidencialiteti, mbi një rrjet me një nivel më të ulët konfidencialiteti (p.sh. "Sensitive" VLAN-e ose Site to Site VPN). IdentiTek siguron mbrojtjen e shkëmbimit të të dhënave mes lokacioneve të ndryshme. Algoritmet e kodimit dhe gjatësia e çelësit duhet të përputhen me politikën ISO-SC-025 Politika e Sigurisë dhe Përputhshmërisë së Menaxhimit të Çelësave të Kodimit

[NET_06] Analiza e lëvizjes së të dhënave në rrjet

Të gjitha flukset e rrjetit, që vijnë nga një rrjet me një nivel më të ulët besimi, duhet të analizohen nga një mekanizëm kontrolli (si antivirus, IDS ose IPS).

Rrjedhat e identifikuara si të rrezikshme nuk pranohen "drop traffic".

Pajisjet e implementuara duhet të garantojnë gjurmueshmërinë e flukseve hyrëse dhe dalëse në internet. Ngjarjet e gjurmuara duhet të regjistrohen dhe regjistrat duhet të ruhen për një periudhë në përputhje me ligjet aktuale.

13.1.3. Ndarja në rrjete

[SGIN_01] Ndarja e rrjetit

Kufijtë ose perimetrat e sigurisë janë të përcaktuar për të ndarë sistemin e informacionit në perimetra me nivele të ndryshme të besimit :

- Interneti: zona të lidhura drejtpërdrejt me Internetin, të pakontrolluara dhe pa nivel besimi.
- Internet LAN: zona me nivel të ulët të besimit e hapur për Internetin.

- DMZ: zona e kontrolluar që ka një nivel të moderuar të besimit. Ajo strehon "host" pajisje që mundësojnë ndërlidhjen mes rrjeteve të brendshme LAN ose Intranetit nga njëra anë dhe Internetit nga ana tjetër, si dhe mbrojtjen e të parëve nga të dytët.
- LAN të brendshme: zona e kontrolluar që ka një nivel të lartë të besimit. Ajo strehon të gjitha burimet e sistemit TI të IdentiTek. Asnjë pajisje nuk duhet të jetë e lidhur drejtpërdrejt me Internetin.

[SGIN_02] Interneti dhe portat e sigurisë

Pajisjet e filtrimit të infrastrukturës janë të implementuara në çdo zonë të ndërseksionit, në mënyrë që të mbrojnë dhe ndajnë rrjetet e brendshme nga ato të jashtme.

Përdorimi i këtyre portave (gateway) e bën menaxhimin e sigurisë së rrjetit më efikas, duke kufizuar rreziqet që do të mund të vinin nga shumëllojshmëria e mënyrave të shkëmbimit të informacionit dhe të aksesimit.

[SGIN_03] Ndarja e rrjetit

Rrjetet lokale ndahen në nën-rrjete për të siguruar ndarjen e pjesëve të ndjeshme dhe për të lejuar kontrollin e incidenteve, nëse është e nevojshme.

Lidhjet janë të filtruara dhe një kontroll hyrjesh aktivizohet në nivelin e nën-rrjetit.

Segmentet e mëposhtme duhet të jenë të ndara: rrjeti i serverëve, rrjeti i përdoruesve, rrjeti i administratës dhe rrjeti i VoIP.

13.2. Transferimi i informacionit

13.2.1. Politikat dhe Procedurat e Shkëmbimit të Informacionit

[IEPP_01] Mbrojtja e shkëmbimit të përdoruesit

Çdo përmbajtje e transmetuar ose marrë nga një përdorues analizohet nga antivirusi.

Përdoruesit që kanë nevojë të shkëmbejnë informacion konfidencial kanë softuer kodimi të ofruar nga IdentiTek në stacionet e tyre të punës. Softueri i kodimit do të përdorë algoritme kodimi në përputhje me politikën ISO-SC-025 Politika e Sigurisë dhe Përputhshmërisë së Menaxhimit të Çelësave të Kodimit

13.2.2. Marrëveshjet për transferimin e informacionit

[EXAG_01] Komunikimi i rregullave të përdorimit të aksesit

Rregullat që rregullojnë shfletimin "browsing" në internet dhe përdorimin e mjeteve të komunikimit u komunikohen të gjithë punonjësve, njihen dhe pranohen. Ata gjithashtu ri-kujtohen gjatë seancave të ndërgjegjësimit për sigurinë.

[PMTR_01] Media fizike në tranzit

Çdo informacion sensitiv i ruajtur në media mbështetëse (CD-ROM, çelës USB, disk i lëvizshëm) është i koduar. Transmetimi fizik i mediave, pajisjeve ose dokumenteve përdor një mbrojtje të përshtatshme, si p.sh. përdorimi i kontenierëve të kyçur, dërgimi me dorë ose paketimi i sigurt me ambalazh kundër ndërhyrjes.

13.2.3. Mesazhet Elektronike

[EMES_01] Serveri i postës elektronike

Shërbimi i emailit IdentiTek trajtohet nga një infrastrukturë e vetme e siguruar nën përgjegjësinë e Departamentit të Teknologjisë dhe Informacionit. Shërbimi i emailit IDENTITEK përdoret vetëm për komunikim të brendshëm. Office 365 përdoret për komunikim të jashtëm.

[EMES_02] Releja e Emaileve ("Email relay")

Përcaktohet një listë e "relays" të autorizuara për t'u lidhur me serverin e postës elektronike, mirëmbahet i përditësuar dhe dorëzohet për autorizim në Departamentin e Teknologjisë dhe Informacionit. Konfigurimi i këtyre serverëve "relays" që përfshin të paktën adresat dërguese dhe marrëse është i përcaktuar, i përditësuar dhe i dorëzuar për autorizim në Departamentin e Teknologjisë dhe Informacionit.

[EMES_03] Formalizimi i rregullave të përdorimit të mesazheve elektronike

Rregullat e formalizuara për përdorimin e mesazheve elektronike në mënyrë të sigurtë dhe pranueshme u jepen përdoruesve.

[EMES_04] Kontrolli i aksesit në mesazhet elektronike

Aksesi në mesazhe kërkon një identifikim dhe vërtetim të përdoruesit përpara se ta përdorë atë.

[EMES_05] Analiza e mesazheve

Mesazhet elektronike (në hyrje) analizohen sistematikisht nga një antivirus me një teknologji të ndryshme nga ajo që përdoret për mbrojtjen e stacioneve të punës dhe serverëve.

[EMES_06] Ridrejtimi i mesazheve

Çdo ridrejtim automatik i mesazheve nga një kuti postare të IdentiTek në një kuti postare të jashtme është i ndaluar.

13.2.4. Konfidencialiteti ose Marrëveshjet e Moszbulimit (Non disclosure agreement)

Të gjithë punonjësit duhet të nënshkruajnë personalisht marrëveshjen e konfidencialitetit të IdentiTek, ndërkohë që kontraktorët (punonjës të përkohshëm, këshilltarë, firma të jashtme për outsourcing, etj.) dhe ofruesit e shërbimeve që përdorin Platformën e IdentiTek duhet të nënshkruajnë personalisht marrëveshjen e mos-zbulimit të IdentiTek. Dhënia e nënshkrimit duhet të ndodhë para fillimit të punës, ose nëse një punonjës ka punuar pa një marrëveshje të mos-zbulimit, duhet të sigurohet një nënshkrim si kusht për vazhdimin e punës. Kjo marrëveshje duhet të rishikohet periodikisht. Kërkesat për marrëveshjen e konfidencialitetit dhe marrëveshjen e mos-zbulimit përfshijnë specifikimet e mëposhtme:

- Përcaktimi i informacionit, llojeve të informacionit ose sistemeve të informacionit që do të mbrohen;
- Kërkesat e konfidencialitetit për atë informacion, në kushte të qarta, të zbatueshme ligjërisht, që përputhen me të gjitha autoritetet përkatëse statutore-rregullatore dhe certifikuese private;
- Përgjegjësitë e nënshkruesve, duke përfshirë kufizimet në përdorimin ose zbulimin e informacionit dhe respektimin e kontrolleve të sigurisë;
- Kushtet e pronësisë së informacionit duke përfshirë çdo sekret tregtar ose kërkesë të pronësisë intelektuale;
- Kohëzgjatja e pritshme e marrëveshjes;
- Veprimet e nevojshme kur marrëveshja përfundon, duke përfshirë kërkesat për kthimin ose shkatërrimin e informacionit;
- E drejta për të monitoruar zbatimin e marrëveshjes;
- Veprimet e pritshme që do të ndërmerren në rast shkeljeje.

14. PËRVETËSIMI, ZHVILLIMI DHE MIRËMBAJTJA E SISTEMEVE TË INFORMACIONIT

Të gjitha sistemet dhe aplikacionet që trajtojnë ose ruajnë informacion sensitiv të IdentiTek, adresojnë kërkesat e sigurisë së informacionit gjatë të gjitha fazave të ciklit të zhvillimit.

14.1. Kërkesat e Sigurisë për Sistemet e Informacionit

14.1.1. Analiza dhe Specifikimi i Kërkesave të Sigurisë

[SRAS_01] Analiza dhe specifikimi i sigurisë

Një vlerësim i veçantë i sigurisë, i ndërmarrë në fazat më të hershme të çdo projekti, lejon, nga çështjet dhe nevojat e formalizuara, të identifikohen rreziqet dhe rreziqet residuale (p.sh. duke marrë parasysh kontrollet e zakonshme të sigurisë të zbatuara) dhe të formalizohen kërkesat e sigurisë dhe kontrollet e sigurisë shtesë që mund të lejojnë rreziqet të reduktohet në një nivel të pranueshëm.

Përgjegjësi i projektit drejton këtë analizë. Drejtori i Departamentit të Teknologjisë dhe Informacionit dhe Menaxheri i Departamentit të Sigurisë të Informacionit informohen për rezultatet.

Për projektet e mëdha, ky studim i sigurisë, duke përfshirë vlerësimin e rreziqeve, miratohet nga Drejtori i Divizionit të Sistemeve të Informacionit të IdentiTek nën këshillimin e Menaxherit të Departamentit të Sigurisë së Informacionit.

[SRAS _02] Formalizimi dhe dokumentimi

Kjo analizë bazohet në një metodologji dhe proces të formalizuar dhe të dokumentuar. Ajo shkruhet në një dokument sigurie që shoqëron projektin dhe do të plotësohet në fazën fillestare të projektit.

[SRAS _03] Blerja e zgjidhjeve teknologjike dhe zhvillimi me shërbime të jashtme

Kërkesat dhe propozimet, për të blerë zgjidhje teknologjike (produkt softueri, sistem ose shërbim) ose për zhvillim, marrin parasysh këtë analizë (SRAS_01).

Kërkesat për propozime (RFP) përfshijnë gjithashtu klauzolat që synojnë të garantojnë qëndrueshmërinë e zgjidhjeve. Ato marrin parasysh kufizimet e mirëmbajtjes dhe evolucionit të sistemeve dhe softuerit mbështetës për shkak të zbatimit të patcheve.

14.1.2. Sistemet e Informacionit të Biznesit

[APP_01] Menaxhimi i Autorizimeve të Aksesit në Aplikacionet e Shoqërisë

Autorizimet e aksesit në aplikacionet e biznesit (caktimi i të drejtave të aksesit, shqyrtimi dhe heqja) bazohen në rregullat dhe procedurat e zbatuara në lidhje me krijimin/modifikimin dhe menaxhimin e të drejtave të qasjes.

Të drejtat e caktuara janë të rishqyrtuara rregullisht.

[APP_02] Kontrolli i Aksesit në Aplikacionet e Shoqërisë

Aksesi në aplikacionet e biznesit është i kontrolluar. Ky kontroll i qasjes bazohet në mekanizmat e zbatuara për identifikimin e përdoruesit, autentifikimin e tyre dhe të drejtat e trashëguara nga profili i tyre dhe nga konteksti i përdorimit.

Këto mekanizma gjithashtu përcaktojnë qasjen në funksionet dhe të dhënat e ndryshme brenda aplikacioneve.

Qasja e caktuar për një përdorues është strikte personale.

[APP_03] Kontrolli i Përdorimit dhe Ndjekja e Aplikacioneve të Shoqërisë

Përdorimet e funksioneve aplikative janë të ndjekura dhe regjistruara (në lidhje me sensitivitetin e tyre dhe të dhënat e aksesuara).

Regjistrat aplikative (logs) analizohen rregullisht për të zbuluar gabimet e përdorimit, mosfunksionim dhe përdorimet e paligjshme.

[WEB_02] Publikimi i të Dhënave në Internet

Informacioni për publikim verifikohet dhe miratohet para se të vendoset “on-line”. Autenticiteti i informacionit “on-line” verifikohet.

Disponueshmëria e informacionit si programe, patch-e ose skedarë konfigurimi është gjithmonë e shoqëruar me sigurimin e integritetit të të dhënave ose mbështjelljen e integritetit që e bën të mundur që një palë e tretë të kontrollojë integritetin e tyre.

14.2. Siguria në Proceset e Zhvillimit dhe Mbështetjes

14.2.1. Procedurat e Kontrollit të Ndryshimeve

[CHCP_01] Procedura formale e kontrollit të ndryshimeve

Çdo ndryshim ndjek procedurën formale të kontrollit të ndryshimeve të vendosur. Procedura e kontrollit të ndryshimeve përfshin identifikimin e ndryshimeve, validimin e ndryshimeve, procesin e kthimit prapa dhe verifikimin e funksionimit të mirë të mjedisit/sistemit të ndryshuar. Kjo procedurë e kontrollit të ndryshimeve është pjesë e menaxhimit të ndryshimeve të zbatuara në IdentiTek.

Çdo ndryshim duhet të miratohet nga Bordi Këshillues i Ndryshimeve (Change Advisory Board).

14.2.2. Rishikimi Teknik i Aplikacioneve pas Ndryshimeve në Sistemin Operativ

[CHCP_02] Rishikime teknike

Para se të aplikohet çdo ndryshim në sistemet operative (Windows, Linux, VMWare), testimi i aplikacioneve të biznesit kryhet me versionin e ri të sistemit operativ. Gjatë këtij testimi, konfigurimi i sigurisë rishikohet dhe përditësohet për të marrë parasysh funksionet e reja të sigurisë të sistemit.

Funksionet dhe shërbimet e sigurisë të zbatuara testohen dhe miratohen para se të implementohen në mjedisin e Prodhimit.

14.2.3. Kufizime në Ndryshimet e Paketave të Softuerit

[ROCSP_01] Procedura formale e kontrollit të ndryshimeve

IdentiTek nuk lejon asnjë ndryshim në paketat e softuerit dhe i përdor këto pa asnjë ndryshim.

14.2.4. Rrjedhja e Informacionit

[INLE_01] Zgjidhje dhe produkte të certifikuara

IdentiTek zgjedh zgjidhje dhe produkte bazuar në kërkesat e sigurisë dhe në produkte ose zgjidhje me certifikim të kritereve të përbashkëta ose certifikim ekuivalent si FIPS.

14.2.5. Parimet e Inxhinierisë së Sigurt të Sistemeve

[SSEP_01] Sistem i Sigurt

IdentiTek i ofron IDEMIA-s (si furnizuesin kryesor të teknologjisë së saj, kontratën e mirëmbajtjes/garancisë), listën e kërkesave specifike të sigurisë për aplikacione, produkte dhe sisteme.

14.2.6. Zhvillimi i Softuerëve të Deleguar

[PDM_03] Zhvillimi i deleguar nga palët e treta

IdentiTek nuk ka zhvillim të deleguar.

14.2.7. Validimi i të Dhënave të Hyrjes (Input data validation)

[CPIA_01] Validimi i të Dhënave të Hyrjes

Kontrollet janë në vende të ndryshme CSO (Zyra e Aplikimeve pranë Gjendjes Civile) për regjistrimin, zyrat qendrore për dokumentet për të verifikuar dhe validuar të dhënat e hyrjes. Çdo

problem me cilësinë e të dhënave ose të dhënat e pasakta zbulohet dhe regjistrohet, dhe transaksioni ndalet për të korrigjuar të dhënat.

14.2.8. Kontrolli i Përpunimit të Brendshëm

[CPIA_02] Funksionimi i mirë i aplikacioneve

Aplikacionet me të dhëna sensitive janë të hostuara në server-a të rinj, të cilët kanë ende suport teknik nga prodhuesi. Kjo politikë është e njëjtë dhe për sistemin operativ.

Kontrollet janë të vendosura për të validuar në zyrat qendrore që të dhënat janë të sakta.

14.2.9. Integriteti i Mesazheve

[CPIA_03] Kontrollet për Integritetin e Mesazheve

Kontrollet e sigurisë janë të vendosura për të siguruar integritetin e mesazhit ose regjistrave gjatë marrjes dhe ruajtjes së mesazheve. Çdo ndryshim i mesazhit zbulohet.

[CPIA_04] Politika e Regjistrimit (“Logging policy”)

Zbatohet një politikë e regjistrimit (“logging policy”), duke specifikuar, për çdo aplikacion, veprimet që duhen audituar, duke mundësuar marrjen e evidencave dhe gjurmëve të nevojshme për trajtimin e incidenteve.

14.2.10. Validimi i të Dhënave të Daljes (Data output validation)

[CPIA_05] Kontrollet e Validimit të të Dhënave të Daljes

Kontrollet operative bëhen në vende të ndryshme, për të validuar rezultatet e aplikacioneve dhe proceseve që vijnë në sistemin TI të IdentiTek, si aplikacionet e biznesit (MorphoCivis, Matcher, MorphoCS) dhe për personalizimin dhe printimin e dokumenteve të identitetit.

[CPIA_06] Testet dhe validimi i funksioneve të sigurisë

Funksionet e sigurisë të mbajtura dhe të zbatuara (funksione në lidhje me prodhimi e dokumenteve) testohen dhe validohen para se të implementohen në prodhim.

14.2.11. Pranimi i Sistemit

[SYAC_01] Pranimi i Sistemit

Kriteret e pranimit të sistemit të ri, përmirësimit dhe versioneve të reja janë të përcaktuara brenda dokumentit të pranimit të testimit që përshkruan:

- Kërkesat për performancë dhe kapacitet kompjuterik;
- Procedurat për rikuperimin e gabimeve dhe rifillimin, dhe planet e “back-up”;

- Përgatitja dhe testimi i procedurave të zakonshme të operimit sipas standardeve të përcaktuara;
- Procedurat manuale efektive;
- Dispozitat për vazhdimësinë e biznesit;
- Dëshmi se instalimi i sistemit të ri nuk do të ndikojë negativisht në sistemet ekzistuese, veçanërisht në kohën e punës më intensive, si në fund të muajit;
- Dëshmi se është kujdesur për efektin që ka sistemi i ri në sigurinë e përgjithshme të organizatës;
- Trajnimi në operacionet ose përdorimin e sistemeve të reja.

14.2.12. Mbrojtja e të Dhënave të Testimit të Sistemit

[PSTD_01] Mbrojtja e mjedisit të testimit

Mjediset e testimit nuk përdorin të dhëna të prodhimit, me përjashtim të mjedisit të testimit të rikuperimit i izoluar plotësisht nga mjedisi i prodhimit i IdentiTek (që teston “backup restore).

14.2.13. Kontrolli i Qasjes në Kodin Burimor të Programit

[ACPS_01] Menaxhimi i burimeve, zhvillimit dhe ndryshimeve

IdentiTek nuk kryen zhvillime software të brendshme.

15. MARRËDHËNIET ME FURNITORËT

Kjo kategori synon të mirëmbaje sigurinë e informacionit të IdentiTek dhe të infrastrukturës së përpunimit të informacionit që aksesohen, përpunohen, komunikohen ose menaxhohen nga palët e jashtme.

15.1.1. Politika e Sigurisë së Informacionit për Marrëdhëniet me Furnizuesit

[Third_01] Identifikimi i rreziqeve që lidhen me palët e jashtme

Para se të lejojë një palë të jashtme të hyjë në ambientet e IdentiTek, Menaxheri i Departamentit të Sigurisë së Informacionit dhe/ose Menaxheri i Sigurisë Fizike, Logjistikes dhe Mirëmbajtjes duhet të analizojë rreziqet e lidhura me këtë projekt dhe të adresojë rreziqet potenciale të identifikuara.

15.1.2. Përcaktimi i Sigurisë me klientët

Të gjitha kërkesat e identifikuara të sigurisë duhet të adresohen para se t'u jepen akses klientëve në informacionin ose asetet e IdentiTek-ut. Konsideratat e kontrollit janë të ngjashme me ato për palët e jashtme.

15.1.3. Përmbajtja e Sigurisë brenda Marrëveshjeve të Furnizuesve

[Third_02] Trajtimi i Sigurisë në Marrëveshjet Kontraktuale

Marrëveshjet e moszbulimit dhe anekset e sigurisë që specifikojnë elementët e mbuluar nga këto marrëveshje përcaktohen gjatë fazave para kontraktore. Këto elementë, të përditësuar nëse është e nevojshme, janë bashkangjitur marrëveshjes të nënshkruar me palët e jashtme. Dispozitat e veçanta përcaktojnë pikat që duhet të merren në konsideratë gjatë përfundimit të kontratës në mënyrë që të garantohet siguria e sistemeve të teknologjisë së informacionit të IdentiTek-ut pas përfundimit të kontratës.

Veçanërisht, ekspozimi i të gjithave ose një pjesë të temave ose specifikimeve të lidhura me personalizimin dhe prodhimin vendoset nën marrëveshjen specifike të Drejtorit Divizionit të Operacioneve të IdentiTek-ut.

Menaxheri i projektit të palës së tretë të jashtme duhet ti drejtojë një kërkesë për akses Drejtorit të Divizionit të Sistemeve të Informacionit të IdentiTek-ut.

Të gjitha akseset e furnitorëve në sistemet e IdentiTek janë të menaxhuara sipas procesit dhe procedurave të kontrollit të aksesit të përcaktuara nga IdentiTek.

Kur fillon shërbimi i palës së jashtme, ekipi i furnitorëve do të marrë një trajnim të ndërgjegjësimit në lidhje me ISMS e IdentiTek. Të gjitha ngjarjet e sigurisë, vulnerabilitetet ose incidentet e zbuluara nga furnitori duhet të raportohen te IdentiTek sipas procesit të ngjarjeve të sigurisë të informacionit.

[Third_04] Zinxhiri i furnizimit të teknologjisë së informacionit dhe komunikimit

Kërkesat për sigurinë e informacionit të aplikuara për blerjen e produkteve dhe shërbimeve të teknologjisë së informacionit dhe komunikimit përcaktohen me furnitorët në anekset e sigurisë.

15.2. Menaxhimi i ofrimit të shërbimeve nga furnizuesit

15.2.1. Ofrimi i Shërbimit

[THIRD_01] Shërbime të palëve të treta

Kërkesat në lidhje me sigurinë e shërbimeve të ofruara nga palët e treta dhe në marrëveshjet e shërbimit janë të formalizuara.

Ato zbatohen, aplikohen dhe mbahen të përditësuara në përputhje me marrëveshjet kontraktuale.

15.2.2. Monitorimi dhe rishikimi i shërbimeve të palëve të treta

[THIRD_02] Monitorimi dhe rishikimi i shërbimeve të palëve të treta

Shërbimet e ofruara nga palët e treta kontrollohen dhe vlerësohen rregullisht. Për këtë qëllim, palët e treta të përgjegjshme për shërbimin e IdentiTek sigurojnë raporte për IdentiTek që të mundësojë këtë kontroll dhe vlerësim.

15.2.3. Menaxhimi i ndryshimeve në shërbimet e palëve të treta

[THIRD_03] Menaxhimi i ndryshimeve në shërbimet e palëve të treta

Ndryshimet në shërbimet e ofruara nga palët e treta vlerësohen dhe menaxhohen.

16. MENAXHIMI I INCIDENTIT TË SIGURISË TË INFORMACIONIT

16.1. Menaxhimi i Ngjarjeve dhe Përmirësimeve të Sigurisë së Informacionit

16.1.1. Përgjegjësitë dhe procedurat

[ISIM_05] Ekipi i alarmit dhe trajtimi i incidentit

Drejtori i Divizionit të Sistemeve të Informacionit të IdentiTek është i ngarkuar për të përcaktuar dhe zbatuar, me mbështetjen e Menaxherit të Departamentit të Sigurisë Fizike, Logjistikës dhe Mirëmbajtjes, Menaxherit të Departamentit të Sigurisë së Informacionit, një ekip të përgjegjës për trajtimin e incidenteve të lidhura me sigurinë e sistemit të informacionit, si:

- Ndërhyrje në rrjet dhe sistem;
- Sulmeve ndaj disponueshmërisë të shërbimit (DDOS);
- Shkeljet e politikës së sigurisë nga përdoruesit.

Ekipi i alarmit është përgjegjës për përcaktimin dhe zbatimin e procedurave të emergjencës, për formalizimin e veprimeve për t'u ndjekur në rast të alarmit për rrethana të veçanta (incidente në prodhim, zbulim të sulmit, shkelje të kontrolleve të hyrjes etj.).

16.1.2. Raportimi i ngjarjeve të sigurisë së informacionit

[ISIM_01] Procedura e raportimit

Drejtorit të Divizionit të Sistemeve të Informacionit të IdentiTek është përgjegjës për të përcaktuar dhe zbatuar një procedurë të formalizuar dhe të dokumentuar për të informuar dhe raportuar për ngjarje dhe vulnerabilitete sensitive që mund të kenë ndikim në sigurinë e aseteve të IdentiTek. Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek është përgjegjës për incidentet e sigurisë së informacionit, ndërsa Menaxheri i Sigurisë Fizike Logjistikës dhe Mirëmbajtjes është përgjegjës për incidentet e sigurisë fizike.

Ne rast të incidenteve kibernetike, Menaxheri i departamentit të Sigurisë së Informacionit të IdentiTek raporton tek AKSK.

[ISIM_02] Raportimi i incidentit nga punonjësit

Punonjësve të IdentiTek-ut u kërkohet të raportojnë, sa më shpejt të jetë e mundur, çdo ngjarje ose dobësi që mund të ndikojë në siguri, tek menaxheri i tij/saj ose tek Departamenti i Sigurisë së Informacionit.

16.1.3. Raportimi i dobësive të sigurisë

[ISIM_03] Monitorimi i sistemeve dhe detektimi i ngjarjeve

Mënyra e organizimit dhe mjetet e monitorimit, mundësoje monitorimin e aktivitetit në nivelin e sistemit të informacionit dhe zbulimin e incidenteve:

- Monitorim i elementeve kritike për qëllime sigurie (viruse, proxy, lidhje celularë, Wi-Fi);
- "Logging" në kohë reale në lidhje me sigurinë e sistemit të informacionit.

Departamenti i Teknologjisë dhe Informacionit ka:

- Detyrë monitorimi të vazhdueshëm të sistemeve dhe rrjeteve dhe shqyrtimin periodik të regjistrave të ndryshëm për të zbuluar çdo anomali nga ku mund të zbulohen incidente;
- Detyre analizimin dhe trajtimin e anomalive të zbuluara. Këto analiza janë formalizuar dhe ruhen dhe regjistrohen.

[ISIM_04] Informacioni dhe ndërgjegjësimi i punonjësve

Çdo menaxher duhet të sigurojë që çdo punonjës ose nën-kontraktor të jetë i sensibilizuar dhe të njohë procedurën e raportimit të incidenteve.

Drejtorit të Divizionit të Sistemeve të Informacionit të IdentiTek është përgjegjës për të përcaktuar planin e trajnimit ndërgjegjësues dhe për të siguruar që plani i trajnimit ndërgjegjësues të implementohet.

16.1.4. Vlerësimi i ngjarjeve të sigurisë së informacionit dhe reagimi ndaj incidentit të sigurisë së informacionit

[ISIM_08] Vlerësimi i ngjarjeve të sigurisë së informacionit

Një ngjarje e raportuar e sigurisë vlerësohet dhe/ose refuzohet ose regjistrohet dhe ndiqet si incident sigurie.

[ISIM_09] Përgjigje ndaj ngjarjeve të sigurisë së informacionit

Përgjigja ndaj një incidenti të sigurisë së informacionit përpunohet nga një procedurë formale e udhëhequr nga Menaxheri i Departamentit të Sigurisë së Informacionit të IdentiTek.

16.1.5. Mësimi nga Incidentet e Sigurisë së Informacionit

[ISIM_06] Mësimi nga incidenti i sigurisë

Çdo incident sigurie kërkon të analizohet për të identifikuar dobësitë e shfrytëzuara dhe për të përcaktuar veprimet e nevojshme korrigjuese për të reduktuar rreziqet e përsëritjes së këtij incidenti (lessons learned).

16.1.6. Mbledhja e evidencave

[ISIM_07] Mbledhja e provave/evidencave

Çdo incident i sigurisë mund të çojë në masë disiplinore, veprim ligjor të kërkuar ose prishje kontrate.

Evidencat dhe elementët të cilët mund të përdoren si prova, që mundësojnë një analizë të specializuar "forensics analysis" të incidentit të sigurisë, mblidhen dhe ruhen në një vend të sigurt.

17. ASPEKTET E SIGURISË SË INFORMACIONIT TË MENAXHIMIT TË VASHDIMËSISË SË BIZNESIT

17.1. Vazhdimësia e sigurisë së informacionit

17.1.1. Përfshirja e sigurisë së informacionit në procesin e menaxhimit të vazhdimësisë së biznesit (BCP)

[BCP_01] Disponueshmëria e BCP - Business Continuity Plan

IdentiTek ka një plan për vazhdimësinë e biznesit që lejon shmangien e ndërprerjeve të zgjatura të sistemeve dhe aplikacioneve kritike. Ky BCP në mënyrë të veçantë përcakton:

- Mjetet dhe kushtet operative të zbatuara që lejojnë sigurimin e funksioneve jetësore të kompanisë pas një situate krize;
- Rolet dhe aktivitetet e secilit;
- Kushtet e kalimit në modalitetin e urgjencës ose zgjidhjet rezervë.

[BCP_02] Përgjegjësia e BCP

Plani i vazhdimësisë së biznesit është nën përgjegjësinë e Drejtorit të Divizionit të Sistemeve të Informacionit të IdentiTek.

[BCP_03] BCP në përputhje me kërkesat e përcaktuara nga shoqëria IdentiTek

Plani i vazhdimësisë së biznesit bazohet në kërkesat e shoqërisë IdentiTek. Ai merr parasysh nevojat e përgjithshme të të gjitha proceseve të biznesit të zbatuara në IdentiTek.

17.1.2. Vazhdimësia e biznesit BCP dhe vlerësimi i rrezikut

[BCP_04] Vlerësimi i rrezikut të BCP

Fazat paraprake të planit të vazhdimësisë së biznesit, duhet të identifikojnë ngjarjet që mund të shkaktojnë ndërprerje në proceset kryesore të biznesit.

17.1.3. Korniza e Planifikimit të Vazhdimësisë së Biznesit

[BCP_05] Disponueshmëria e ambienteve të ruajtjes së “back-ups”

IdentiTek ka një vend ruajtjeje të jashtme rezervë që mundëson ruajtjen e mediave rezervë që përmbajnë informacione kritike.

[BCP_06] Vendndodhja e ruajtjes rezervë (back-up)

Vendi ruajtjes rezervë (back-up) është mjaftueshëm larg vendit qendror për të adresuar rreziqet kryesore fizike dhe mjedisore.

[BCP_07] Përkufizimi i elementeve të shpëtuar

Lista e informacionit për transferim dhe koha e lejuar për transferim ruhet. Kjo listë shqyrtohet gjatë zbatimit të çdo aplikacioni të ri dhe të paktën një herë në vit.

17.1.4. Testimi, mirëmbajtja dhe rivlerësimi i planeve të vazhdimësisë së biznesit

[BCP_08] Përditësimi i BCP

Integrimi i një aplikacioni të ri në sistemin e informacionit shkakton përditësimin e planit të vazhdimësisë së biznesit nëse është e nevojshme.

[BCP_09] Testimi i BCP

Plani i vazhdimësisë së biznesit testohet dhe vërtetohet të paktën një herë në vit.

17.2. Tepricat

17.2.1. Disponueshmëria e Objekteve të Përpunimit të Informacionit

[BCP_10] Disponueshmëria

Sistemi i informacionit i ngarkuar me përpunimin është plotësisht “redundant” (pajisjet e rrjetit, pajisjet e sigurisë, pajisjet e serverëve, ...) në mënyrë që të përputhet me kërkesat e disponueshmërisë së biznesit.

18. PËRPUTHSHMËRIA

18.1. Përputhshmëria me Kërkesat Ligjore

18.1.1. Identifikimi i Ligjeve të Zbatueshme

[COMP_01] Përputhshmëria me kërkesat ligjore dhe rregullatore

Procedurat e sigurisë të vendosura, si dhe përditësimet e tyre, organizohen në mënyrë që të respektojnë kërkesat ligjore, rregullatore dhe kontraktuale.

Një dokument i quajtur "kërkesat ligjore: politika e qeverisjes së sigurisë" ofron tekstet e lidhura me të gjitha kërkesat ligjore dhe rregullat e ndryshme.

[COMP_02] Identifikimi i legjislacionit aktual

Kryhet një monitorim për të identifikuar ligjet dhe rregullat kombëtare ose ndërkombëtare që Teknologjia e Informacionit e IdentiTek duhet të respektojë. Këto ligje dhe rregulla identifikohen dhe dokumentohen.

18.1.2. Drejtat e Pronës Intelektuale (IPR)

[COMP_03] Të Drejtat e pronës intelektuale

IdentiTek ka rregulla dhe procedura të përshtatshme për të garantuar të drejtat e pronës intelektuale për asetet e saj.

Përveç kësaj:

- IdentiTek angazhohet të blejë çdo produkt softuer nga burime të njohura;
- Licencat origjinale dhe dëshmitë e blerjes së pajisjeve dhe softuerëve mbahen në vend të sigurt;
- Kryhet rregullisht një kontroll për të verifikuar respektimin e legjislacionit dhe për të siguruar që licencat janë të blera.

18.1.3. Mbrojtja e Regjistrave Organizative

[COMP_04] Kërkesat për mbrojtjen e regjistrave organizative

Kontrollet organizative dhe teknike janë të përcaktuara dhe të zbatuara për të mbrojtur regjistrat e rëndësishëm për arsye ligjore ose rregullatore (regjistrat e auditimit, aktivitetet e pajisjeve të kontrollit të qasjes dhe arkivat e monitorimit video) nga humbja, shkatërrimi dhe falsifikimi, në përputhje me kërkesat ligjore.

18.1.4. Privatësia dhe Mbrojtja e të Dhënave Personale të identifikueshme

[COMP_05] Mbrojtja e të Dhënave Personale të identifikueshme

IdentiTek ka implementuar kontrolle për të mbledhur, procesuar dhe shpërndarë të Dhëna Personale të identifikueshme. Divizioni i Sistemeve të Informacionit ka përgjegjësinë për të mbajtur dhe për të mbrojtur këto të dhëna, sipas përcaktimeve në legjislacionin përkatës.

18.1.5. Parandalimi i Abuzimit të Pajisjeve të Përpunimit të Informacionit

[COMP_06] Parandalimi i abuzimit të sistemit TI të IdentiTek

Kontrolle teknike janë të përcaktuara dhe të zbatuara për të monitoruar aktivitetet brenda sistemit të Teknologjisë së Informacionit të IdentiTek. Regjistrat mblidhen, ruhen dhe shqyrtohen rregullisht.

Në çdo tentative autentifikimi mesazhet paralajmëruese shfaqen në ekran që tregojnë se kompjuterët duhet të aksesohen vetëm nga përdorues të autorizuar.

18.1.6. Rregullimi i Kontrolleve Kriptografike

[COMP_07] Rregulimi i kontrolleve kriptografike

Ekziston një proces për të verifikuar përputhshmërinë e kërkesave rregullatore lokale në lidhje me kontrollet kriptografike . Ky proces kryhet nga shoqëria IdentiTek për:

- Importin e pajisjeve dhe softuerit kompjuterik për kryerjen e funksioneve kriptografike;
- Importin e pajisjeve dhe softuerit kompjuterik që është i projektuar për të shtuar funksione kriptografike;

18.2. Përputhshmëria me Politikat dhe Standardet e Sigurisë, dhe Përputhshmëria Teknike

18.2.1. Përputhshmëria me Legjislacionin dhe Standardet e Sigurisë

[POL_06] Përputhshmëria me Legjislacionin

Politika e sigurisë e përcaktuar nga IdentiTek përputhet me Legjislacionin Shqiptar si me poshtë:

Ligji Nr. 25, datë 21.3.2024, “Për Sigurinë Kibernetike”’;

Ligji Nr.107,datë 1.1.2015 “Për Identifikimin Elektronik dhe Shërbimet e Besuara”, i ndryshuar;

Ligji Nr. 9880, datë 25.2.2008, “Për Nënshkrimin Elektronik”, i ndryshuar;

Ligji Nr. 43/2023 “Për Qeverisjen Elektronikei ndryshuar.

Ligji Nr. 124/2024 "Për Mbrojtjen e të Dhënave Personale"

Menaxheri i Departamentit të Sigurisë së Informacionit është përgjegjës për kontrollimin periodik të faqes zyrtare të AKSK për të evidentuar ndryshime në legjislacionin në fuqi dhe për të ndjekur reflektimin e përditësimeve në politikat e Shoqërisë IdentiTek brenda një afati kohor të arsyeshëm.

Përputhshmëria me udhëzimet, direktivat e tjera që lidhen me fushën e veprimit të Shoqërisë IdentiTek janë të transpozuara gjithashtu të plota në dokumentin "Deklarata e Zbatueshmërisë së ISMS në IdentiTek (SOA)", në përputhshmëri me kërkesat e Standardit ISO 27001:2022

[POL_07] Përputhshmëria me politikat dhe standardet e sigurisë

Perimetri i IdentiTek ISMS duhet të përputhet me standardin ISO 27001:2022.

Çdo procedure rishikohet të paktën një herë çdo 2 vjet dhe në çdo rishikim nga zotëruesi i procedurës, për të siguruar përputhshmërinë e trajtimeve të informacionit me politikat e sigurisë. Në rast të mos përputhjes, zotëruesi identifikon shkaqet, vlerëson kërkesën për të nisur veprime për të parandaluar ketë mos përputhje, implementon veprimin korrigjues dhe rishikon veprimin korrigjues në vijim.

18.2.2. Kontrolli i Përputhshmërisë Teknike

[VUL_01] Analiza e cënueshmërisë

Për të verifikuar përputhjen me standardet e lidhura me implementimin e sigurisë, realizohet një fushatë auditimi të cënueshmërisë "Penetration Testing", të paktën një herë në çdo 2 vjet. Këto analiza të cënueshmërisë përfshijnë elementët e mëposhtëm:

- Eksplorimi i mundësive të qasjes nga një stacion i zakonshëm i lidhur në rrjetin administrativ të brendshëm të IdentiTek.
- Eksplorimi i mundësive të qasjes në infrastrukturën e Teknologjisë së Informacionit të IdentiTek nga një sistem i lidhur me rrjetin e internetit pa autorizim specifik (Back box pen test).
- Analiza "grey box" ose "white box" në pjesë të zgjedhura të sistemit të informacionit të IdentiTek.

Këto teste përfshijnë, si teste automatike të kryera me mjete të dedikuara (zbulimi automatik i cënueshmërive), ashtu edhe teste manuale. Testet manuale duhet të kryhen nga individë të specializuar të ndryshëm nga ata që janë të përgjegjshëm për administrimin e përditshëm të infrastrukturave. Këto analiza kryhen nga njerëz me njohuri të larta.

Rezultatet e testimit të cënueshmërive analizohen nga Divizioni i Sistemeve të Informacionit dhe Departamenti i Sigurisë të Informacionit të IdentiTek. Cënueshmëritë e identifikuara krijojnë nevojën për plane veprimesh në mënyrë që të trajtohen këto cënueshmëri.

---------- Fundi i dokumentit ----------