

HYRJE

Informacioni, është një burim për ALUIZNI-in, pa të cilin pothuajse të gjitha aktivitetet tona do të ishin të pamundura.

Informacioni përfshin: klientet (popullin), sistemet, dhe të dhënat e legalizimeve; të dhënat administrative, të dhënat e personelit dhe të dhënat financiare; rrjetin e brendshëm kompjuterik, sistemet e bazës së të dhënave; analiza; publikime dhe referenca.

Informacioni mund të ekzistojë në shumë forma. Mund të jetë i printuar, i shkruar në letër, i ruajtur në forme elektronike. Ai mund të transmetohet me postë ose me mjete elektronike, paraqitur në filmime apo prezantime, ose mund të transmetohet nëpërmjet një bisede. Çfarëdo forme të këtij informacioni apo në çfarëdo mënyre të jetë ai, ALUIZNI merr masat për mbrojtjen maksimale të tij.

ALUIZNI duhet të perpiqet të bëjë gjithçka që mundet për të mbrojtur asetet e tij të informacionit në mënyra që janë të përshtatshme dhe efektive. Kjo e ndihmon ALUIZNI-in për të përmbushur përgjegjësitë e tij dhe për t'i mundësuar stafit një veprimtari normale dhe të sigurt.

Aftësia jonë për të marrë, zhvilluar, analizuar dhe publikuar dhe për të mbrojtur të dhënat tona do të na mundësojë ngritjen e një reputacioni, si një institucion i cili i jep rëndësi maksimale mbrojtjes së sigurisë së informacionit, duke zbatuar rigorozisht direktivat e standardeve ndërkombëtare ISO 27001 dhe direktivave të vendosura nga Komisioneri për Mbrojtjen e Të Dhënave Personale.

OBJEKTIVA

Objektivi i sigurisë është që të mbrojmë ALUIZNI-in nga problemet e sigurisë së informacionit që mund të kenë një efekt negativ në operacionet tona dhe gjendjen tonë profesionale, si dhe në reputacionin tonë si institucion.

Problemet e sigurisë mund të përfshijnë konfidencialitetin (individin, marrjen apo dhenien e informacioneve shpjeguese të papërshtatshme), integritetin (informacioni të ndryshohet qëllimisht ose gabimisht) dhe disponueshmërinë (informacioni nuk është në dispozicion kur është i nevojshme). Një përkufizim i gjerë i sigurisë, do të përdoret për të përfshirë të gjitha llojet e incidenteve që perbejne nje kercenim per perdorimin efektiv te informacionit.

PËRDORIMI

Përdorimi i të gjitha masave të arsyeshme, të përshtatshme, praktike dhe efektive të sigurisë për të mbrojtur proceset e rëndësishme dhe aktivitetin për arritjen e objektivit të sigurisë.

Përdorimi i ISO /IEC 27002: 2013: Teknologji informacioni - Teknikat e sigurisë - Kodi i Praktikës për Menaxhimin e Sigurisë së Informacionit.

Vazhdimisht shqyrtojmë përdorimin e masave të sigurisë, në mënyrë që te përmirësojmë mbrojtjen institucionale.

Mbrojmë dhe menaxhojmë asetet e informacionit, gjë e cila mundeson përmbushjen e detyrimeve kontraktuale, legjislative, reputacionin dhe përgjegjësite etike. Si një institucion që ofron shërbime kombëtare, jemi të vetëdijshëm për nevojën e mbrojtjes së sigurisë së informacionit, si dhe për transparencën që duhet të kemi me publikun.

PËRGJEGJËSITË

I gjith personeli i përhershëm dhe i përkohshëm, i ALUIZNI-t ka detyrimin të mbrojtë pasuritë e informacioneve, sistemet dhe infrastrukturën. Ata, në çdo kohë, veprojnë në një mënyrë të përgjegjshme, profesionale të sigurtë, të vetëdijshme dhe që përputhet me këtë politikë

Gjithkush do të respektojë asetet e informacionit të palëve të treta. Një mbrojtje e tillë kërkohet me kontratë, me ligj ose nga ana etike.

Punonjësit e ALUIZNI-t janë përgjegjës për identifikimin e mangësive të sigurisë në praktikën dhe/ose përmirësimet që mund të bëhen në politikën tona ekzistuese të sigurisë.
Raportimi i tyre behet në Sektorin e IT-së.

Identifikimi i rreziqeve të sigurisë së informacionit me prioritet, duke u përgjigjur menjëherë, duke zbatuar masat mbrojtëse të cilat janë të përshtatshme, efektive dhe praktike.

Të gjithë punonjësit e ALUIZNI-t janë përgjegjës për veprimet e tyre në lidhje me sigurinë e informacionit.

Të gjitha informacionet (duke përfshirë informacionet e palës së treta), do të jenë të mbrojtur nga kontrollet e sigurisë dhe procedurat e trajtimit të informacioneve sensitive.

Kur është e nevojshme nga marrëveshjet kontraktuale apo nga urdhri i gjykatës ose prokurorisë, informacioni do të jepet për institucionet apo shoqëritë nga ALUIZNI, duke firmosur një marrëveshje konfidencialiteti.

Incidentet aktuale ose veprimet që dyshohen të jenë si incident i sigurisë së informacionit IT, raportohen menjëherë në Sektorin e IT-së, ku menaxhohen incidentet, analizohen shkaqet, si dhe nxirren mesime se çfarë do të bëhet që të mos ndodhin në të ardhmen.

PERSONAT PËRGJEGJËS

Përfaqësuesit e ALUIZNI-t krijojnë këtë Politikë të Sigurisë së Informacionit dhe angazhohen në zbatimin e saj. Ata mundësojnë shqyrtimin vjetor të saj nga Sektori i Teknologjisë së Informacionit.

Kjo politikë rishikohet për plotësinë, efektivitetin dhe përdorshmërinë. Efektiviteti matet me aftësinë e ALUIZNI-t për të shmangur incidentet e sigurisë dhe për të minimizuar ndikimet që rezultojnë.

Drejtori i Përgjithshëm i ALUIZNI-t si dhe Përgjegjësi i Sektorit IT, do të nënshkruajnë të gjitha versionet e reja të Politikës së Sigurimit të Informacionit.

Punonjësit e ALUIZNI-t janë përgjegjës për identifikimin e mënyrave në të cilat Politika e Sigurimit të Informacionit të mund të permiresohet. Sugjerimet për permiresim, duhet të dërgohen pranë Sektorit IT.

Nëqoftëse ndryshimet duhen bërë në mënyrë të menjëhershme, kërkohet një takim i vecantë me menaxherin e sigurisë së informacionit, përndryshe sugjerimet do të diskutohen në takimin e rishikimit vjetor të Politikës.

NDËRGJEGJËSIMI

Një kopje e kësaj politike do të vihet në dispozicion për të gjithë personelin e punësuar aktualisht, ose kur ata fillojnë punë pranë ALUIZNI-t. Seksione individuale të politikës do të jenë të përditësuara si dhe do të jenë të publikuara në faqen e web-it të ALUIZNI-t.

Të gjithë punonjësit si dhe institucionet shtetërore apo kompanitë private që kanë bashkepunim me ALUIZNI-n pritët të jenë në djeni të kësaj politike, si dhe të veprojnë në përputhje me të në çdo kohë.

Përgjegjësi i Sektorit IT, ka përgjegjësinë për interpretimin dhe sqarimin e Politikës së Sigurimit të Informacionit. Çdo punonjës që kërkon informacion

të mëtejshëm mbi çdo aspekt të kësaj politike duhet të diskutojë nevojat e tij me përgjegjës të Sektorit të IT-së.

FUSHA E ZBATIMIT

Kjo politikë zbatohet për të gjithë punonjësit e ALUIZNI-t, institucionet shtetërore apo kompanite private dhe atyre që përdorin objektet dhe informacionin e saj. Pajtueshmëria me Politikën do të jetë pjese e kontrates së punësimit.

Mospërputhja me Politikën e Sigurisë së Informacionit përbën shkelje dhe do të trajtohet si një çështje disiplinore. Përgjegjësi i Sektorit të IT-së, ka përgjegjësinë për vendimet lidhur me zbatimin e kësaj politike, duke përdorur procedurat disiplinore në dispozicion të tij/saj, si të jetë më e përshtatshme.

ALUIZNI do të inkurajojë miratimin dhe përdorimin e kësaj Politike të Sigurisë së Informacionit nga palët e treta që bashkëpunojnë në siper marrjet e përbashkëta.

Drejtori i Përgjithshëm

Z. Artan Lama

