UNIVERSITETI "UKSHIN HOTI" PRIZREN
UNIVERSITY "UKSHIN HOTI" PRIZREN
Rruga e Shkronjave Nr. 1, 20000
Prizren, Republika e Kosovës
www.uni-prizren.com

RREGULLORE
PËR SHËRBIMET E TEKNOLOGJISË SË INFORMACIONIT (TI)

Prizren, 2022

Në mbështetje të nenit 23 paragrafi 1.2 dhe 1.3 të Statutit të UPZ–së dhe në pajtim me Ligjin për Arsimin e Lartë të Republikës së Kosovës, Këshilli Drejtues i Universitetit në mbledhjen e mbajtur me datën 23.05.2022, miraton:

Rregullore për Shërbimet e Teknologjisë së Informacionit (TI)

Neni 1
Qëllimi dhe fushëveprimi

1. Qëllimi i kësaj Rregulloreje është të përcaktojë kriteret dhe kushtet që duhet të plotësojë Universitetit për organizimin dhe për funksionimin e sistemeve të tyre të teknologjisë së informacionit (në tekstin e mëposhtëm TI-së), të cilat mundësojnë uljen e rrezikut operacional që mund të shkaktohet nga keqpërdorimi i sistemeve të TI-së si dhe të ruajë besueshmërinë e këtyre sistemeve në mbështetjen e veprimtarisë së Universitetit.
2. Kjo rregullore aplikohet në Universitet.

Neni 2
Përkufizimet

1. Të gjitha termet në këtë rregullore kanë të njëjtin kuptim me termet e definuara në legjislacionin përkatës në fuqi, ose / dhe përkufizimeve në vijim për qëllimin e kësaj rregulloreje:

   1.1. **Universiteti** – Universiteti "Ukshin Hoti" Prizren

   1.2. **Klient** – menaxhmenti i Universitetit, anëtarët e Këshillit Drejtues, stafi i rregullt dhe i angazhuar akademik, stafi administrativ, dhe studentët.

   1.3. **Sistemi i informacionit** – nënkupton një grup i tërësishëm teknologjik që përbëhet nga infrastruktura (komponentët softuerike dhe harduerike), organizatat, njerëzit dhe procedurat për mbledhjen, ruajtjen, përpunimin, transmetimin, shfaqjen dhe përdorimin e të dhënave dhe informacionit;

   1.4. **Komponentët e softuerit** - nënkupton të gjitha llojet e sistemit operativ, softueri aplikativ, veglat e zhvillimit të softuerit dhe sisteme tjera softuerike;

   1.5. **Komponentët e harduerit** - nënkuptojnë pajisjet kompjuterike, pajisjet e rrjeteve kompjuterike, mediumet për ruajtjen e të dhënave dhe pjesa tjetër e pajisjeve teknike që shërbejnë si mbështetje për funksionimin e sistemeve të informacionit;

   1.6. **Përdoruesit e sistemit të informacionit** - nënkuptojnë të gjithë personat që janë të autorizuar për të përdorur sistemet e informacionit (studentët, të punësuarit me orar të plotë, të punësuarit me orar të pjesshëm, stafi vizitor, përdoruesit mysafir, studentët që vijnë nga programi i shkëmbimit);

1.7. **Ofruesi i jashtëm i shërbimit** - nënkupton personin fizik apo juridik, i cili në bazë të një marrëveshjeje të shkruar i ofron shërbim Universitetit nga jashtë;

1.8. **Asete** - nënkupton informacionet (siç janë bazat e të dhënave, kontratat dhe marrëveshjet, dokumentimi i sistemeve, informacionet e hulumtimeve, manualët e shfrytëzuesve, materialet e trajnimit, procedurat e operimit ose të përkrahjes, planet e vazhdimësisë së aktivitet mësimorit, gjurmët e auditimit dhe informacionet e arkivuara); Asetet softuerike (aplikacionet softuerike, sistemet softuerike, veglat e zhvillimit, etj..); Asetet fizike (pajisjet kompjuterike, pajisjet e komunikimit, pajisjet e lëvizshme (ang. Removable media) dhe pajisjet e tjera.); Shërbimet (shërbimet kompjuterike dhe ato të komunikimit, shërbimet e përgjithshme); Personeli (së bashku me kualifikimet, shkathtësitë dhe eksperiencën) ;Të paprekshme (si reputacioni i Universitetit).

1.9. **Tavolinë e pastër** – nënkupton largimin e të gjithë dokumenteve dhe aseteve të tjera konfidenciale nga tavolina e punës gjatë periudhës së pambikëqyrur dhe në përfundim të orarit të punës.

Neni 3
Menaxhimi i teknologjisë së informacionit

1. Menaxhimi i teknologjisë së informacionit duhet të përfshijë kërkesat si në vijim:

   1.1. Të ketë funksionalitetin, kapacitetin dhe performancën që të ofrojnë mbështetje që kërkohet nga proceset e aktiviteve mësimore;

   1.2. Ofron kontrollë të përshtatshme të validimit të të dhënave, gjatë procesit të përpunimit, dhe gjatë nxjerrjes së të dhënave, për të parandaluar pasaktësi dhe mospërputhje në të dhëna dhe informacione;

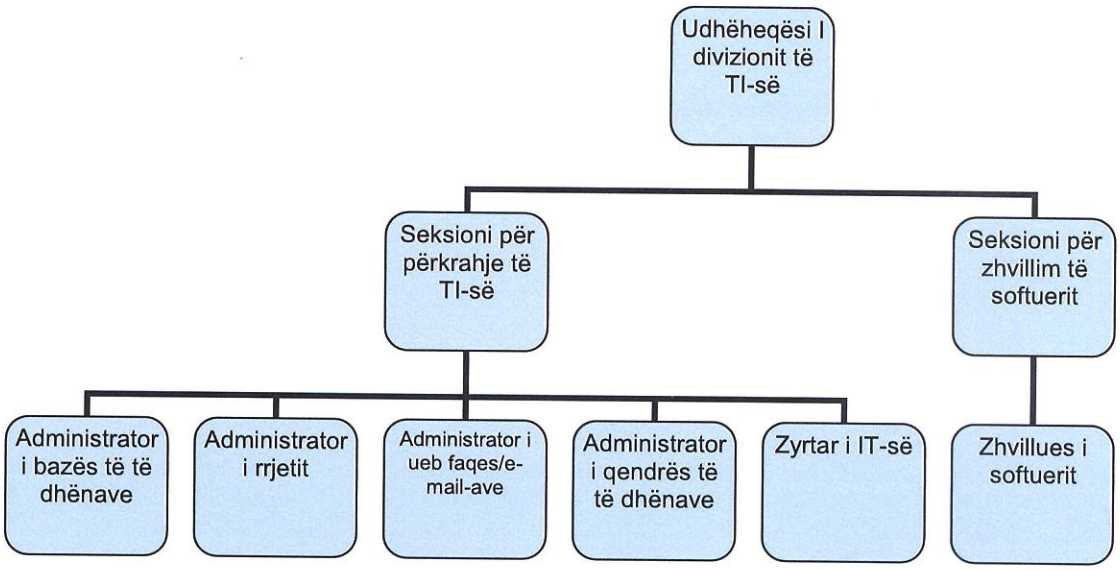
   1.3. Ofron informacion në kohë të saktë dhe të plotë ,për marrjen e vendimeve të aktivitet të mësimorit dhe menaxhimin e rrezikut, për të mundësuar siguri dhe funksionim të qëndrueshëm të Universitetit;

2. Universiteti, do të bëjë monitorimin, rregullimin dhe përmirësimin e vazhdueshëm të procesit të menaxhimit të TI-së, për të zvogëluar ekspozimin ndaj rrezikut dhe duke ruajtur sigurinë dhe funksionalitetin e tij.

Neni 4
Struktura organizative për menaxhimin e TI-së

1. Universiteti, duhet të themelojë strukturë organizative të njësisë së TI-së (divizioni i TI-së) me staf të mjaftueshëm në numër dhe të përshtatshëm, për të siguruar që fusha e TI-së menaxhohet në mënyrë efikase. Ndarja e detyrave duhet të bëhet sipas standardit ISO IEC 20000-1 me përgjegjësi dhe kompetenca të përcaktuara qartë për procesin e menaxhimit të TI-së. Kjo njësi duhet të dokumentojë raporte të rregullta informuese së paku në baza tre mujore për menaxhmentin e lartë të Universitetit.

2. Ky divizion ka këtë strukturë:



1. Udhëheqësi i divizionit
   i. Administrator i bazës të të dhënave,
   ii. Administrator i rrjetit,
   iii. Administrator i ueb faqes/e-mail-ave,
   iv. Administrator i qendrës të të dhënave,
   v. Zhvilluesi i softuerit,
   vi. Zyrtar i IT-së

Divizioni i TI-së është përgjegjës për këto shërbime:

2.1. Ofrim të qasjes në shërbime të postës elektronike zyrtare (e-mail) për klientët. Ky shërbim ofrohet duke u bazuar në udhëzimin administrativ nr. 04/2010 për shfrytëzimin e postës elektronike zyrtare në institucionet e Republikës së Kosovës (shtojca nr.1)

2.2. Ofrim të shërbimeve përkrahëse (*help desk*) për klientët në lidhje me përdorimin e softuerit dhe harduerit dhe është i bazuar në udhëzimin administrativ nr. 03/2010 për përdorimin e softuerit dhe harduerit (shtojca nr.3)

2.3. Ofrim të shërbimeve të mirëmbajtjes së ueb-faqes zyrtare. Ky shërbim është i bazuar në udhëzimin administrativ nr. 01/2011 për përdorimin e Internetit në institucionet e Republikës së Kosovës (shtojca nr.4)

3. Në rastin e delegimit të funksioneve të TI-së tek ofruesi i jashtëm i shërbimit (kontrakutes), Universiteti duhet të caktojë së paku një punonjës të brendshëm të specializuar në fushën e teknologjisë së informacionit, si përgjegjës për koordinimin dhe mbarëvajtjen e funksioneve të TI-së.
4. Universiteti, duhet të përcaktojë personin përgjegjës për sigurinë e informacionit, i cili duhet të menaxhojë sigurinë e sistemit të informacionit dhe të koordinojë politikat dhe proceset për sigurinë e informacionit lidhur me funksionet dhe platformat teknologjike.

Neni 5
Politikat dhe procedurat për menaxhimin e TI-së

1. Divizioni i TI-së është përgjegjës për miratimin e politikave të teknologjisë dhe sigurisë së informacionit dhe në baza vjetore duhet të vlerësojë përshtatshmërinë e politikave dhe të kryejë rishikimin e tyre.
2. Universiteti ,përcakton objektiva, strategji dhe kërkesa të sigurisë, për veprimtarinë e sistemeve të TI-së, përcakton politikat për teknologji dhe siguri të informacionit, si dhe procedura për proceset e fushës. Këto procedura duhet të miratohen nga Këshilli Drejtues i Universitetit.
3. Universiteti në përputhje me strategjinë e aktivitet mësimorit miraton strategji për zhvillimin e sistemeve të TI-së.
4. Në rast se Universiteti siguron të gjithë ose një pjesë të veprimtarisë (ose të sistemeve) së tij ,pra të TI-së ofrues të jashtëm të shërbimit, atëherë Universiteti miraton procedurë të brendshme për delegimin e funksioneve për sigurimin e përputhshmërisë me kërkesat e kësaj rregulloreje për siguri dhe për mirëfunksionim të këtyre sistemeve.
5. Procedura e brendshme për delegimin e funksioneve sipas paragrafit 4 të këtij neni duhet të përfshijnë së paku, elementet si në vijim:
   5.1. Identifikimin e funksioneve që do të delegohen dhe vlerësimin e ndikimit që do të ketë delegimi i atyre funksioneve;
   5.2. Procedurat për delegimin e funksioneve, përfshirë kriteret për përzgjedhjen e pranuesit të funksioneve të deleguara;
   5.3. Afatet dhe metodat e raportimit të pranuesit të funksioneve të deleguara, tek Universiteti;
   5.4. Mënyrat e monitorimit të pranuesit të funksioneve të deleguara, nga ana e Universitetit;
6. Politikat dhe procedurat për menaxhimin e TI-së duhet të përcaktojnë së paku elementet në vijim:
   6.1. Administrimi dhe operimi i sistemeve të TI-së;

6.2. Struktura organizative për menaxhimin e TI-së;

6.3. Infrastruktura harduerike e fushës së TI-së (diagramet e konfigurimeve);

6.4. Klasifikimi i dokumentacionit dhe mbrojtja e sisteme dhe të dhënave;

6.5. Backup-i të dhënave të sistemeve;

6.6. Menaxhimi i ndryshimeve të sistemeve;

6.7. Menaxhimi i incidenteve;

6.8. Menaxhimi i rrezikut të sistemeve të TI-së;

6.9. Përcaktimi i mekanizmave të sigurisë së sistemeve të TI-së;

6.10. Menaxhimi i palëve të treta.

Neni 6
Zhvillimi dhe prokurimi i sistemeve të TI-së

1. Për të minimizuar rrezikun, Universiteti duhet të ndjek trendin e zhvillimeve të softuerëve duke u përkujdesur që të shfrytëzoj vetëm versionet e azhurnuara dhe të mbështetura nga ofruesit e tyre.
2. Universiteti miraton procedura të brendshme për mënyrën se si realizon zhvillimet, ndryshimet dhe testet në sistemet e saj të TI-së. Sistemet e TI-së vendosen në operim *live*, vetëm pasi punonjësi i specializuar që realizon verifikimin e zbatueshmërisë së procedurave dhe të mirëfunksionimit të sistemeve të japë miratimin e tij të dokumentuar.
3. Ofruesi i jashtëm i shërbimit gjatë implementimit dhe punës në sisteme nuk duhet në asnjë mënyrë të ketë qasje në versionet e sistemit që janë në prodhim (*live*) përveç qasjeve vetëm për lexim (*read only*) me aprovim të veçantë dhe mbikëqyrje nga ana e Universitetit. Kontraktorët dhe palët e tjera të jashtme duhet që të gjitha ndryshimet t'i testojnë në një ambient testues.

Neni 7
Delegimi i funksioneve të TI-së tek ofrues të jashtëm të shërbimit

1. Universiteti është përgjegjëse për të siguruar që aktiviteti i TI-së kryhet në përputhje me të gjitha kërkesat e përcaktuara me këtë rregullore edhe në rastet ku i gjithë ose një pjesë e aktivitetit të TI-së, sigurohet nga ofrues i jashtëm i shërbimit të TI-së.
2. Para përzgjedhjes së ofruesit të jashtëm të shërbimit të TI-së Universiteti duhet të ndërmarrë aktivitetet si në vijim:

   2.1. Kryerjen e vlerësimit të rrezikut të operacioneve të Universitetit që mund të lindin nga përdorimi i shërbimit të jashtëm të ofruar gjatë procesimit të aktiviteteve të Universitetit;

   2.2. Përcaktimin e standardeve minimale që ofruesi i jashtëm i shërbimit të TI-së duhet

të përmbushë dhe të cilat duhet të harmonizohen me planin e vazhdimësisë së aktivitet mësimorit;

2.3. Përcaktimin e masave të nevojshme për shmangien e konfliktit të interesit;

2.4. Përcaktimin e mënyrës së monitorimit të shërbimit dhe kualitetit të operimit të kompanisë, situatës financiare dhe profilin e rrezikut përmes testimit periodik të pajtueshmërisë me politikë e sigurisë së sistemit të informacionit;

2.5. Të bëjë vlerësimin e duhur të veprimtarisë së ofruesit të jashtëm të shërbimit të TI-së nga aspekti ligjor dhe financiar si dhe nga aspekti i mënyrës se si menaxhon sigurinë e sistemit të informacionit të përcaktuar në këtë rregullore;

2.6. Përcaktimin e menaxhimit të koordinuar të incidenteve të sigurisë.

3. Marrëveshja në mes Universitetit dhe ofruesit të jashtëm të shërbimit të TI-së duhet të përcaktohet përmes kontratës së shkruar e cila ndër të tjera duhet të përfshijë:

3.1. Të dhënat e palëve të ndërlidhura (Universiteti dhe ofruesi i jashtëm i shërbimit të TI-së);

3.2. Të drejtat dhe detyrimet e palëve të ndërlidhura;

3.3. Përshkrimin e funksioneve të deleguara;

3.4. Afatet kohore të ofrimit të shërbimit;

3.5. Marrëveshja e nivelit të shërbimit;

3.6. Angazhimin e ofruesit të shërbimit të TI-së për të kryer veprimtarinë e tij në përputhje me legjislacionin në fuqi, kërkesat, rregullatorët si dhe politikat e miratuara nga Universiteti;

3.7. Periudhën e njoftimit për përfundimin e kontratës e cila është e mjaftueshme për gjetjen e zgjidhjeve alternative;

3.8. Trajtimin dhe ruajtjen e konfidencialitetit të të dhënave;

3.9. Dispozitë që përcakton se ofruesi i jashtëm i shërbimit të TI-së, do t'i nënshtrohet mbikëqyrjes nga ana e Universitetit lidhur me aktivitetet e deleguara të TI-së;

3.10. Detyrimin e ofruesit të jashtëm të shërbimit të TI-së ,për të informuar menjëherë Universitetin për çdo fakt që mund të ketë një ndikim të rëndësishëm në aftësinë e tij, për të kryer në mënyrë efikase dhe efektive veprimtarinë e tij sipas kërkesave ligjore në fuqi;

3.11. Të drejtën e Universitetit për t'u informuar në lidhje me mbarëvajtjen e funksioneve të deleguara nga ofruesi i jashtëm i shërbimeve të TI-së, si dhe të drejtën e Universitetit për të dhënë udhëzime të përgjithshme apo të veçanta në lidhje me kryerjen e funksioneve të deleguara;

3.12. Të drejtën e Universitetit, të inspektojë dhe kontrollojë veprimtarinë e ofruesit të

jashtëm të shërbimit të TI-së lidhur me aktivitetet e deleguara të TI-së.

4. Ofruesi i jashtëm i shërbimit nuk mund t'i nënkontraktojë shërbimet përveç nëse është përcaktuar në marrëveshjen bazë të lidhur në mes Universitetit dhe këtij ofruesi të shërbimit.

5. Universiteti është e obliguar të menaxhojë rreziqet që rrjedhin nga marrëdhëniet kontraktuale me ofruesit e jashtëm të shërbimit, aktivitetet e të cilëve kanë të bëjnë me sistemin e informacionit që është në përdorim nga Universiteti. Universiteti është e obliguar të monitorojë vazhdimisht metodën dhe cilësinë e aktiviteteve të kontraktuara nga ofruesi i jashtëm.

Neni 8
Menaxhimi i rrezikut për sistemet e informacionit

1. Universiteti vendos kritere për rrezikun e lejueshëm në lidhje me përdorimin e sistemeve të saj të TI-së sipas standardeve të ISO 27005.

2. Të paktën një herë në vit ose në çdo rast ndryshimesh të rëndësishme të kërkesave të sigurisë së TI-së, Universiteti kryen analiza të rrezikut të sistemeve të TI-së për të siguruar që ky rrezik mbahet brenda kufijve të pranueshëm lidhur me veprimtarinë e Universitetit. Rezultatet e analizës së rrezikut dokumentohen.

3. Menaxhimi i rrezikut të sistemit të informacionit duhet të përfshijë të gjithë sistemin e informacionit të Universitetit të integruar në të gjitha fazat e zhvillimit të tij.

4. Menaxhimi i rrezikut të sistemit të informacionit duhet të përfshijë planin vjetor të vetëdijësimit të punonjësve të Universitetit për përdorimin adekuat të shërbimeve të ofruara përmes sistemit të informacionit të Universitetit.

Neni 9
Siguria e sistemeve të informacionit

1. Siguria e sistemeve të TI-së do të bazohet në përcaktimin e përmbushjes së kritereve të mëposhtme:

   1.1. Konfidencialiteti: informacioni duhet të jetë i qasshëm vetëm për përdoruesit e autorizuar;

   1.2. Integriteti: ruajtje e saktësisë dhe plotësisë së sistemit të informacionit;

   1.3. Disponueshmëria: qasje në çdo kohë në sistemin e TI-së për përdoruesit e autorizuar.

2. Universiteti duhet të menaxhojë në vazhdimësi procesin e sigurisë së sistemit të informacionit.

3. Universiteti duhet të identifikojë dhe monitorojë nevojat për sigurinë e sistemit të informacionit, të paktën duke u bazuar në rezultatet e vlerësimit të rrezikut të atij sistemi

dhe detyrimet që lindin nga aktet e brendshme apo marrëdhëniet kontraktuale.

4. Universiteti duhet të përcaktojë kriteret, metodat dhe procedurat për klasifikimin e informacionit sipas shkallës së ndjeshmërisë dhe kritikalitetit - në lidhje me pasojat e mundshme të shkeljes së konfidencialitetit, integritetit të tyre dhe disponueshmërisë.
5. Siguria e informacionit dhe të gjitha aktivitetet që ndërlidhen me të, duhet të jenë në pajtueshmëri me të gjitha ligjet në fuqi që kanë të bëjnë me informacionin dhe operacionet e institucionit.

Neni 10
Siguria fizike e sistemeve të informacionit

1. Universiteti duhet të ndërmarr masa të nevojshme të mbrojtjes për të ndaluar çdo qasje fizike të pa autorizuar, ndërhyrje apo dëmtim i informatave, pajisjeve procesuese të informatave dhe operacioneve të Universitetit, bazuar në standardin ISO 27002.
2. Universiteti duhet të krijojë procedura të qasjes dhe punës për zonat e sigurisë për të gjithë punonjësit dhe palët e jashtme. Zonat e sigurisë duhet të jenë të mbrojtura përmes kontrolleve të qasjes për të siguruar që vetëm punonjësit e autorizuar të kenë qasje.
3. Pajisjet duhet të mirëmbahen për t'u mbrojtur nga dështimet, për të siguruar disponueshmëri të vazhdueshme e integritet dhe të mbështeten nga ndërprerjet si rezultat i dështimeve të pajisjeve ndihmëse, katastrofave natyrore, sulmeve keqdashëse, apo aksidentale etj.
4. Masat e sigurisë duhet të caktohen edhe për pajisjet e përdorura dhe vendosura jashtë objekteve të Universitetit varësisht prej lokacionit dhe duhet të merren në konsideratë rreziqet gjatë përcaktimit të kontrolleve të nevojshme.
5. Të gjitha pajisjet që përmbajnë informacion duhet të verifikohen për të siguruar se të gjitha të dhënat dhe softuerët e licencuar janë larguar para hedhjes, shkatërrimit ose ripërdorimit, për të pamundësuar rikthimin e informacionit origjinal.
6. Të gjithë shfrytëzuesit duhet të vetëdijesohen për kërkesat e sigurisë dhe procedurat për mbrojtjen e pajisjeve të pa mbikëqyrura.
7. Universiteti duhet të përcaktojë kritere, metoda dhe procedura për tavolinë të pastër me qëllim të mbrojtjes së informacionit.
8. Obligimet kontraktuale për punonjësit dhe ofruesit e jashtëm të shërbimit të TI-së duhet të reflektojnë politikat e Universitetit për sigurinë e informacionit. Të gjithë punonjësit dhe ofruesit e jashtëm të shërbimit të TI-së duhet të kuptojnë përgjegjësitë për rolet që konsiderohen.
9. Ku është e përshtatshme për aplikim, Universiteti do të përcaktojë se punonjësit dhe ofruesit e jashtëm të shërbimeve do të ruajnë informacionin e marrë gjatë ushtrimit të veprimtarisë së tyre edhe për një periudhë të caktuar pas ndërprerjes së marrëveshjes

kontraktuale me punonjësin apo ofruesit e jashtëm të shërbimit të TI-ve.

10. Universiteti ,duhet të përcaktojë veprimet dhe masat që duhet të ndërmarrë në rast të shkeljes së kërkesave të sigurisë nga punonjësit ose ofruesit e jashtëm të shërbimit të TI-së.

Neni 11
Menaxhimi i aseteve të TI-së

1. Universiteti duhet të identifikojë të gjitha asetet e TI-së.
2. Universiteti duhet të mbajë inventarin e të gjitha aseteve me të gjitha informacionet e nevojshme, duke përfshirë këtu tipin e asetit, formatin, lokacionin, informacionet mbi backup-in (aty ku është i aplikueshëm), informacionet mbi licencën dhe vlerën për aktivitetin mësimor.
3. Universiteti duhet të përcaktojë dhe dokumentojë pronësinë dhe klasifikimin e të gjitha aseteve të lidhura me procesimin e informacioneve.
4. Pronari i asetit do të jetë përgjegjës për:
   4.1. Të siguruar se informacionet dhe asetet e lidhura me procesimin e informacioneve janë të klasifikuar sipas ndjeshmërisë;
   4.2. Të përcaktojë dhe rishikojë rregullisht kufizimet në qasje dhe klasifikimin.
5. Universiteti duhet të përcaktojë rregullat mbi përdorimin e pranueshëm të informacioneve dhe aseteve të lidhura me procesimin e informacioneve.

Neni 12
Menaxhimi i rrjeteve kompjuterike

1. Rrjeti kompjuterik i Universitetit duhet të menaxhohet dhe kontrollohet me qëllim të mbrojtjes së informacionit të sistemeve dhe aplikacioneve. Universiteti duhet të implementojë kontrollë për të siguruar mbrojtjen e konfidencialitetit dhe integritetit të informacionit në rrjet dhe mbrojtjen e shërbimeve nga qasjet e pa autorizuara bazuar në standardin ISO 27002.
2. Për menaxhimin e rrjetave kompjuterike Universiteti duhet të përcaktojë:
   2.1. Procedura për përdorimin dhe menaxhimin e shërbimeve dhe pajisjeve të rrjetit me qëllim të kufizimit të qasjeve në shërbimet e rrjetit dhe aplikacionet;
   2.2. Vendosjen e kontrollave të veçanta për mbrojtjen e konfidencialitetit dhe integritetit të të dhënave që kalojnë përmes rrjeteve publike ose pa tela;
   2.3. Teknologjinë e aplikuar për sigurinë e shërbimeve të rrjetit si autentikimi, enkriptimi dhe kontrollet e lidhjeve në rrjet;
   2.4. Grupet e shërbimeve të informacionit, shfrytëzuesit dhe sistemet e informacionit duhet të izolohen nga rrjetat publike;

2.5. Kontrolla të veçanta duhet kushtuar qasjeve të ofruesve të jashtëm të shërbimit në rastet e nevojës për ndërlidhje (me palët e treta).

Neni 13
Menaxhimi i qasjes së përdoruesve

1. Universiteti do të menaxhojë qasjet në sistemet e informacionit përmes procedurave të brendshme përkatëse për menaxhimin të drejtave për qasje të përdoruesve. Procedurat e brendshme duhet të përmbajnë kritere për qasje, autorizim, identifikim dhe vërtetim të përdoruesve sipas standardeve ISO27001.
2. Çdo shfrytëzues duhet të jetë unik dhe sistemi duhet të përcaktojë kriteret e vendosjes së fjalëkalimit sipas standardeve ISO 27000. Para dhënies së qasjes në sistemet e informacionit, si punëtorët e brendshëm të Universitetit edhe ofruesit e jashtëm të shërbimit, duhet të nënshkruajnë një marrëveshje për ruajtjen e konfidencialitetit dhe mos zbulimit të informacionit.
3. Universiteti duhet të sigurohet që autorizimi i qasjes së përdoruesve në sistemet e informacionit të bëhet nga personat përgjegjës të atyre sistemeve dhe të bazohet në parimin e qasjes më të ulët të mundshme në sistem, duke mundësuar kryerjen e detyrave të punës. Universiteti, duhet që së paku në baza 6 mujore të rishikojë të drejtat e qasjes së përdoruesve në sistemet e rëndësisë së lartë, bazuar në vlerësimin e rrezikut dhe së paku në baza vjetore të gjitha sistemet tjera.
4. Në menaxhimin e të drejtave të qasjes së përdoruesve, Universiteti duhet që në mënyrë veçantë të autorizojë qasje të privilegjuar dhe/ose qasjet nga larg në sistemin e informacionit. Të gjitha qasjet dhe aktiviteti i përdoruesve të privilegjuar dhe qasjet nga larg duhet të monitorohen.
5. Qasjet nga larg në sistemet e informacionit duhet të mundësohen me metodat për autentikim dy-faktorësh. Komunikimi mes pajisjes që do të qaset në sistemin e informacionit nga larg duhet të ketë të vendosura masat e enkriptimit *skaj-në-skaj* për çdo seancë të komunikimit.
6. Universiteti duhet të monitorojë dhe ruaj ngjarjet e sigurisë së informacionit në infrastrukturën e tyre duke u bazuar në ISO 27001.

Neni 14
Auditimi i brendshëm i sistemit të informacionit

1. Kërkesat e përcaktuara nga Rregullorja për kontrollet e brendshme dhe auditimin e brendshëm zbatohen për auditimin e sistemit të informacionit.
2. Veprimtaria e fushës së TI-së duhet t'i nënshtrohet së paku rishikimit periodik vjetor që fokusohet në metodologjinë e bazuar në rrezik.
3. Auditimet e TI-së duhet të kryhen nga personat kompetentë në kuadër të funksionit

të auditimit të brendshëm ose nga persona të jashtëm të kontraktuar për këtë qëllim.

Neni 15
Ruajtja e informacionit

1. Ruajtja e informacionit (backup) duhet të bëhet sipas procedurave të brendshme të Universitetit.
2. Aktet e brendshme sipas paragrafit 1 të këtij neni duhet të përmbajnë së paku elementet si në vijim:
   2.1. Caktimin e nivelit të nevojshëm të backup-it të informacionit;
   2.2. Mbajtjen të dhënave të sakta dhe të kompletuara mbi backup-in e informacioneve, si dhe procedurat e dokumentuara të rikthimit të backup-ëve;
   2.3. Llojin (ang. Full, incremental, differential) dhe frekuencën e backup-ëve sipas kompleksiteti të aktivitet mësimorit.
3. Orari i krijimit të backup-ëve duhet të caktohet duke u siguruar që të gjithë informacionet dhe softueri do të mund të rimëkëmben në rast të fatkeqësive ose dështimit të pajisjeve.
3. Backup-ët duhet të ruhen në një lokacion të dytë, në një distancë të mjaftueshme për të mos qenë të rrezikuar nga kërcënime të njëjta me lokacionin qendror.
4. Backup-ëve duhet t'u jepet niveli i duhur i mbrojtjes fizike dhe mjedisore, në përputhje me standardin e aplikuar në lokacionin qendror.
5. Backup-ët duhen të testohen rregullisht, duke siguruar që ato janë të besueshme dhe të shfrytëzueshme kur nevojiten.
6. Backup-ët duhen të mbrohen nga qasjet e pa autorizuara përmes enkriptimit.
7. Kohëzgjatja e ruajtjes së informacionit duhet të bëhet sipas legjislacionit në fuqi.
8. Çdo shërbim i kontraktuar i nënshtrohet rregullave të njëjta të ruajtjes së informacionit që vlejnë për shërbimet e brendshme (jo të kontraktuara) të Universitetit.

Neni 16
Qendra e të Dhënave

1. Kërkesat e përcaktuara nga Udhëzimi adminsitrativ nr.01/2010-MAP mbi sigurinë për qasjen ,Rregullorja për kërkesat minimale të sigurisë zbatohen për qendrën e të dhënave.
2. Përveç kërkesave nga paragrafi 1 të kësaj rregulloreje, Universiteti duhet të përcaktojë kushtet e qasjes së personelit dhe palëve të treta të autorizuara për qasje në dhomën e serverëve në rast të urgjencave.
3. Dhoma e serverëve duhet të jetë e kufizuara për qasje vetëm për personelin e

autorizuar dhe të monitorohet përmes evidentimit të hyrje / daljeve të stafit dhe personave të jashtëm në këto hapësira.

Neni 17
Vazhdimësia e operimit në situata të jashtëzakonshme

1. Me qëllim të funksionimit të pandërprerë të të gjitha sistemeve të TI-së, Universiteti duhet të krijojë një proces për punë të vazhdueshme.
2. Universiteti duhet të aprovojë një plan që do të analizojë ndërprerjen e aktiviteteve, e që së paku do të përmbajë:
   2.1. Proceset që janë më me prioritet si dhe resurset e nevojshme për këto procese;
   2.2. Aktivitetet finale që do të duhet të arrihen (Service Delivery Objective);
   2.3. Kohën e fundme të rimëkëmbjes (Recovery Time Objective);
   2.4. Pika e fundme e kthimit (Recovery Point Objective).
3. Universiteti duhet të miratojë në baza vjetore Planin e Vazhdimësisë së Aktiviteteve, si dhe Planin e Rimëkëmbjes nga Fatkeqësitë, i cili rregullon krijimin e kushteve për rimëkëmbjen dhe disponueshmërinë e resurseve të sistemit të informacionit ,të nevojshme për të kryer proceset kritike të aktiviteteve.
4. Plani i Vazhdimit të Aktivitetit të mësimorit dhe ai i rimëkëmbjes nga fatkeqësitë duhet të përfshijë së paku kërkesat në vijim:
   4.1. Procedurat që duhet ndërmarrë në rast të ndërprerjes së funksionimit të sistemeve;
   4.2. Një listë të përditësuar të të gjitha resurseve të nevojshme njerëzore dhe teknike për të rivendosur vazhdimësinë e aktivitet mësimorit;
   4.3. Informacion në lidhje me personat përgjegjës dhe zëvendësit e tyre të cilët do të jenë përgjegjës për rimëkëmbjen e operacioneve në rast të ngjarjeve të paparashikuara, duke përfshirë detyrat e tyre të përcaktuara dhe përgjegjësitë, si dhe planin e linjave të brendshme dhe të jashtme të komunikimit;
   4.4. Një lokacion alternativ në rast të ndërprerjes së aktiviteteve mësimore dhe rimëkëmbjes në funksion proceseve të aktivitet mësimor në lokacionin primar. Ky lokacion duhet të ketë distancën e duhur nga qendra primare, me qëllim të shmangies së ndikimit të rreziqeve të njëjta në të dy lokacionet.
5. Për zbatimin e planeve sipas paragrafit 4 të këtij neni Universiteti do të sigurojë që të gjithë punonjësit të njihen me rolet dhe përgjegjësitë e tyre në raste urgjente.
6. Universiteti do të harmonizojë planet me ndryshimet e shërbimeve të TI-së, duke përfshirë ndryshimet në produktet, aktivitetet, proceset dhe sistemet, me ndryshimet në mjedis, si dhe me politikën dhe strategjinë e shërbimeve të TI-së.
7. Universiteti do të testojë planet, së paku një herë në vit dhe pas shfaqjes së

ndryshimeve të rëndësishme, dhe do të dokumentojë rezultatet e këtyre dhe testeve.

8. Në menaxhimin e vazhdimësisë së shërbimeve të TI-së, Universiteti merr parasysh aktivitetet që u janë besuar palëve të treta dhe varësinë nga shërbimet e këtyre palëve.

Neni 18
Dokumentimi i veprimtarisë së TI-së

Universiteti mban dokumentacion e plotë dhe të përditësuar të organizimit, të pajisjeve, të sistemeve, të qasjeve dhe të faktorëve të tjerë të rëndësishëm që lidhen me veprimtarinë e TI- së. Një dokumentacion i tillë ,do të provojë se përputhshmëria me kërkesat e kësaj rregulloreje është e vazhdueshme.

Neni 19
Masat përmirësuese

Çdo shkelje e dispozitave të kësaj rregulloreje do të jetë subjekt i masave përmirësuese dhe ndëshkuese siç përcaktohen rregullore për procedurat dhe masat për përpunimin dhe sigurinë e të dhënave personale.

Neni 20
Hyrja në fuqi

Kjo rregullore hyn në fuqi ditën e miratimit nga Këshilli Drejtues i Universitetit "Ukshin Hoti" Prizren.

Prof. Asoc. Dr. Arif Murrja

Kryesues i Këshillit Drejtues