Tbilisis humanitaruli saswavlo universiteti
TBILISI HUMANITARIAN TEACHING UNIVERSITY

თბილისის ჰუმანიტარული სასწავლო უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები

დამტკიცებულია:	შპს თბილისის ჰუმანიტარული სასწავლო უნივერსიტეტის აკადემიური საბჭოს დადგენილება N10 20.05.2019
შეტანილია ცვლილება:*	აკადემიური საბჭოს დადგენილება N07 02.05.2025 მოდიფიცირებულია თჰუაკადემიური საბჭოს 2025წლის03 სექტემბრის N14 გადაწყვეტილებით

* - შეტანილი ცვლილების აღწერა წარმოდგენილია დანართი 1-ში

1. თჰუ-ს ინფორმაციული ტექნოლოგიების პოლიტიკა

1.1. თბილისის ჰუმანიტარული სასწავლო უნივერსიტეტის (თჰუ) მიერ ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა და მისი მართვა აღიარებულია საქმიანობად, რომელიც საჭიროა უნივერსიტეტის ძირითადი ბიზნესსაქმიანობისათვის, ქონების დაცვისა და დაწესებულების ფინანსური სიცოცხლისუნარიანობის უზრუნველყოფისათვის.

1.2. თბილისის ჰუმანიტარული სასწავლო უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა ეფუძნება უნივერსიტეტის სტრატეგიული განვითარების გეგმას, რომლის მიხედვით დასახულია ამოცანა 1.5. ინფორმაციული ტექნოლოგიების ინფრასტრუქტურისა და ა დმინისტრირების გაუმჯობესება.

1.3. წარმოდგენილი დოკუმენტი განსაზღვრავს ინფორმაციული ტექნოლოგიების მართვის ხელშეწყობ მექანიზმებს უნივერსიტეტის ფორმისა და ფუნქციების შესაბამისად.

1.4. თჰუ-ში ფუნქციონირებს ინფორმაციული ტექნოლოგიების სამსახური, რომელიც უზრუნველყოფს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის (კომპიუტერული ტექნიკა, პროგრამული უზრუნველყოფა, ინტერნეტი) მუდმივ და სტაბილურ ხელმისაწვდომობას სტუდენტებისა და პერსონალისათვის.

1.5. ინფორმაციული ტექნოლოგიების სამსახური მოქმედებს საკუთარი დებულებისა და უნივერსიტეტის ბიზნესპროცესების უწყვეტობის გეგმის შესაბამისად.

1.6. უნივერსიტეტში დანერგილია ელექტრონული სერვისები და მართვის ელექტრონული სისტემები, რომლებიც უზრუნველყოფენ მომსახურებისა და პროცესების მართვას.

2. ინფორმაციული ტექნოლოგიების მართვის პროცედურები

2.1. კომპიუტერული რესურსები

2.1.1. კომპიუტერული ტექნიკა ჩართულია ინტერნეტში 24/7 რეჟიმით, როგორც პერსონალისათვის განკუთვნილ სამუშაო ოთახებში, ასევე ბიბლიოთეკის სამკითხველო დარბაზებში და კომპიუტერულ კლასებში.

2.1.2. ყველა კომპიუტერი აღჭურვილია ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ რეკომენდირებული და დაყენებული ანტივირუსული პროგრამული უზრუნველყოფით. ანტივირუსული ბაზების განახლება ხორციელდება ცენტრალიზებულად.

2.1.3. ინფრასტრუქტურაზე მუდმივ ზედამხედველობას უწევს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური, რომელიც მომხმარებელთა მხრიდან შემოსული განცხადებების საფუძველზე ახორციელებს კომპიუტერული ტექნიკის მდგომარეობის შესწავლას და საჭიროების შესაბამისად იღებს გადაწყვეტილებას დაზიანებული სისტემების შეკეთებისა და ახლით ჩანაცვლების შესახებ.

2.2. კომპიუტერული და ციფრული შენახვის მოწყობილობების ელექტრონულ მონაცემთა დაცვის მექანიზმები

2.2.1. უნივერსიტეტის საკუთრებაში არსებული ყველა კომპიუტერისა და ციფრული შენახვის მოწყობილობის გადაადგილების, შეკეთების, ჩამოწერისა თუ აღდგენის დროს აუცილებელია დაცულ იქნას უნივერსიტეტის ელექტრონული მონაცემები და მათი კონფიდენციალურობა;

2.2.2. ყველა კომპიუტერი და ციფრული შენახვის მოწყობილობა ინფორმაციის დამუშავებისათვის უნდა მიეწოდოს ინფორმაციული ტექნოლოგიების სამსახურს;

2.2.3. კომპიუტერებისა და ციფრული შენახვის მოწყობილობების დამუშავების დროს უნდა წაიშალოს მოწყობილობებზე უნივერსიტეტთან დაკავშირებული ყველა მონაცემები და ლიცენზირებული პროგრამული უზრუნველყოფა ან ფიზიკურად განადგურდეს თვით მოწყობილობა.

2.3. ინფორმაციული ტექნოლოგიების ქსელი

2.3.1. უნივერსიტეტის კორპუსები, ბიბლიოთეკა და სამკითხველო დარბაზი უზრუნველყოფილია უსადენო წვდომის ქსელით.
2.3.2. ინტერნეტ მომსახურებას უწევს 2 ინტერნეტ-პროვაიდერი. ორივე მომწოდებლიდან ინტერნეტის მიღება ხდება ოპტიკურ-ბოჭკოვანი არხის საშუალებით.
2.3.3. უნივერსიტეტში მოწყობილია ზოგადი სტანდარტის შესაბამისი საუნივერსიტეტო ქსელი (Router -> Firewall -> ვარსკვლავური ტოპოლოგიის ლოკალური ქსელი). საკაბელო ქსელით დაფარულია უნივერსიტეტის მთელი ტერიტორია.

2.4. უსადენო ქსელების მართვის, მონიტორინგისა და ექსპლოატაციის მექანიზმები

2.4.1. უსადენო ქსელების მართვა, მონიტორინგი და ექსპლუატაცია ხდება ინფორმაციული ტექნოლოგიების სამსახურის მიერ.
2.4.2. უსადენო ქსელში დაშვება შეიძლება იყოს თავისუფალი ან შეზღუდული;
2.4.3. უსადენო ქსელთან დასაკავშირებელ პაროლებს ადგენს ინფორმაციული ტექნოლოგიების სამსახური.
2.4.4. თავისუფალი დაშვების უსადენო ქსელის პაროლი შეიძლება გაენდოს ნებისმიერ მსურველს, დაიწეროს საინფორმაციო დაფაზე ან განთავსდეს ნებისმიერ თვალსაჩინო ადგილზე.
2.4.5. შეზღუდული წვდომის უსადენო ქსელის პაროლი გაენდობა მხოლოდ საზოგადოების იმ წევრებს რომელთაც სამსახურეობრივი საქმიანობიდან გამომდინარე სჭირდებათ აღნიშნულ ქსელთან წვდომა და ისინი ვალდებული არიან საინფორმაციო ტექნოლოგიების სამსახურის თანხმობის გარეშე სხვას არ გაანდონ პაროლი.
2.4.6. კომპიუტერული ქსელის მონიტორინგის ფარგლებში ინფორმაციული ტექნოლოგიების სამსახური უფლებამოსილია შეამოწმოს და განიხილოს მისი კომპიუტერული სისტემებისა და ქსელების ყველა მხარე, მათ შორის ინდივიდუალური სესიებისა და ანგარიშის ფაილები. შემოწმების მიზანია გამოავლინოს კომპიუტერული ქსელის პრობლემები, ვირუსები და სხვა საზიანო პროგრამები, დაადგინოს, არღვევს თუ არა მომხმარებელი უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას ან სახელმწიფო კანონმდებლობას.
2.4.7. უნივერსიტეტის ქსელისა და ინტერნეტის შემოწმების უფლებამოსილმა პერსონალმა არ უნდა გაამჟღავნოს ქსელის მონიტორინგის პროცესში მიღებული ინფორმაცია უნივერსიტეტის ადმინისტრაციის ნებართვის გარეშე.
2.4.8. ინფორმაციული ტექნოლოგიების სამსახურის მიერ ჩატარებული კომპიუტერული ქსელის მონიტორინგის ჩანაწერები ინახება ანალიზის მიზნით.
2.4.9. მომხმარებელმა პატივი უნდა სცეს სხვა მომხმარებელთა უფლებებს მის მონაცემებთან დაკავშირებით და არ უნდა განახორციელოს ან სცადოს ქსელის მონიტორინგი.

2.5. ინფორმაციულიუსაფრთხოების ინციდენტები

2.5.1. უნივერსიტეტი ვალდებულია განახორციელოს უსაფრთხოების ინციდენტების იდენტიფიცირება, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას.

2.5.2. უნივერსიტეტს ინფორმაციული ტექნოლოგიების სისტემის ფუნქციონირებაზე პასუხისმგებელი პირები პერიოდულად წარმოადგენენ ანგარიშს ინფორმაციული უსაფრთხოების ინციდენტების, მათი წყაროების (შიდა, გარე) მათი ფორმების (DDoS, Keylog და სხვა) მიხედვით, გამოსწორებისა და ოპტიმიზაციის რეკომენდაციებთან ერთად.

2.6. კომუკიკაციებისა და ოპერაციების მართვა;

უნივერსიტეტი ახორციელებს მუდმივ კონტროლს ინფორმაციის დამამუშავებელ მოწყობილობებზე მათი სწორი და უსაფრთხო სარგებლობის უზრუნველყოფის მიზნით;

2.7. ვირუსებისგან დაცვა

2.7.1. უნივერსიტეტი ახორციელებს შესაბამის კონტროლს, რათა თავიდან იქნეს აცილებული ვირუსების გავრცელება უნივერსიტეტს შიგნითდა უნივერსიტეტის მიზეზით– მის გარეთ; სისტემები, აპლიკაციები და მონაცემთა სარეზერვოასლები;

2.8. ვებ-გვერდისა და ოფიციალური FB-გვერდის ადმინისტრირების პროცედურები

2.8.1. უნივერსიტეტის ოფიციალური ვებ-გვერდი www.thu.edu.ge ასრულებს საკომუნიკაციო და საინფორმაციო ფუნქციას და მასზე ქართულ და ინგლისურ ენებზე განთავსებულია საკონტაქტო და სხვა საჭირო ინფორმაცია.

2.8.2. ვებ-გვერდის ადმინისტრატორი რეგულარულად ახორციელებს ვებ-გვერდისა და FB-გვერდის ინფორმაციის განახლებას, ისე, რომ დაცულია ინფორმაციის გონივრულ ვადაში მიღების ინტერესი.

2.8.3. ვებ-გვერდის ადმინისტრატორი ქმნის საერთო საინფორმაციო სივრცეს (ბუფერს), რომელშიც ინფორმაციის განთავსება ხდება მხოლოდ უნივერსიტეტის ადმინისტრაციის (რექტორი, ვიცე- რექტორი, ადმინისტრაციის ხელმძღვანელი, ხარისხის უზრუნველყოფის სამსახურის უფროსის, ფაკულტეტის დეკანების) და სტრუქტურული ერთეულების ხელმძღვანელების მიერ მოწოდებული ინფორმაციის საფუძველზე.

2.8.4. ვებ-გვერდის ადმინისტრატორი შესრულებული სამუშაოს შესახებ ინფორმაციას ელექტრონულად უგზავნის დავალების გამცემ პირს.

2.9. ელექტრონული ბაზების ადმინისტრირების პროცედურები

2.9.1. თჰუ-ს გააჩნია ელექტრონული ბაზა - www.thu.ge, საიდანაც ხორციელდება სასწავლო პროცესის მართვა ელექტრონულად.

2.9.2. ელექტრონული ბაზების ადმინისტრირების პროცედურების სახელმძღვანელო დოკუმენტია სასწავლო პროცესის მართვის ელექტრონული სისტემის ფუნქციონირების მექანიზმები, რომელიც დამტკიცებულია შპს თბილისის ჰუმანიტარული სასწავლო უნივერსიტეტის აკადემიური საბჭოს დადგენილებით N4 09.03.2019. იხ. დანართი 2.

დანართი 1

ცვლილებების შეტანის აღწერა

#	დადგენილების # და თარიღი	ცვლილების ისტორია

დანართი 2

სასწავლო პროცესის მართვის ელექტრონული სისტემის ფუნქციონირების მექანიზმები (გვ. 5)