აკაკი წერეთლის სახელმწიფო უნივერსიტეტი

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები

შექმნის თარიღი: 01.03.2018
განახლების თარიღი:
შემდეგი განახლების თარიღი:

ცვლილებები

№	თარიღი	შენიშვნა

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის განხილვა და განახლება ხდება ყოველწლიურად.

შედგენილია: **საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ**

დამტკიცებულია: **უნივერისტეტის აკადემიური საბჭოს მიერ დადგენილება №65 (17/18) 01.03.2018**

ქუთაისი, 2018 წ.

შინაარსი

განმარტებები

უნივერსიტეტის საზოგადოება – უნივერსიტეტის სტუდენტები, ფაკულტეტის სასწავლო-სამეცნიერო აკადემიური პერსონალი, თანამშრომლები, კონსულტანტები, ხელშეკრულებით მოწვეული და უნივერსიტეტის მიერ დამატებით სხვა საჭიროების მიხედვით განსაზღვრული ადამიანთა ჯგუფები;

ინფორმაცია – საგნების, ფაქტების, მოვლენების, ცნებებისა და იდეების შესახებ ცოდნა, რომელიც გარკვეულ კონტექსში ღებულობს აზრს;

აპარატურული უზრუნველყოფა – გამოთვლითი სისტემების ელექტრონული და მექანიკური ნაწილები;

პროგრამული უზრუნველყოფა – ინფორმაციის დამუშავებისათვის საჭირო პროგრამების, პროცედურების, წესებისა და შესაბამისი დოკუმენტაციის ერთობლიობა;

კომპიუტერული ქსელი და ქსელური მოწყობილობები – ელექტრონულ-ტექნიკური მოწყობილობების (ქსელური ადაპტერი, მარშრუტიზატორი, კომუტატორი, კონტენტრატორი და სხვა) საშუალებით შექმნილი მონაცემთა ურთიერთგაცვლის სისტემა;

ინფორმაციული ტექნოლოგიები – ინფორმაციის წარმოდგენის, დამუშავების, შეგროვების, შენახვისა და ძებნის ურთიერთდაკავშირებული სამეცნიერო, ტექნოლოგიური, საინჟინრო მეცნიერებათა ერთობლიობა. ინფორმაციული ტექნოლოგიები მოიცავს ინფორმაციის დამუშავების აპარატურულ-პროგრამულ უზრუნველყოფასა და საკომუნიკაციო საშუალებებს;

კომპიუტერული (გამოთვლითი) რესურსები – უნივერსიტეტის საკუთრებაში და/ან ზედამხედველობის ქვეშ არსებული ყველა აპარატურული და პროგრამული უზრუნველყოფა, სადენიანი და უსადენო კომპიუტერული ქსელი და ქსელური მოწყობილობები;

საინფორმაციო რესურსები – უნივერსიტეტის მიერ შექმნილი/დამუშავებული/შენახული/გადაცემული ინფორმაცია. ზოგადად, წერილები, განცხადებები, ბრძანებები, დოკუმენტები და სხვ.

კომპიუტერი – სამუშაო სადგური, სერვერული, სამაგიდო, პორტარტული გამოთვლითი მოწყობილობა;

სერვერი – სპეციალურად გამოყოფილი აპარატურული ან/და პროგრამული უზრუნველყოფა, რომელიც განსაზღვრავს სხვა მოწყობილობების/პროგრამების ფუნქციონირებას. არსებობს: მონაცემთა ბაზის, ფაილური, ინტერნეტის, სამომხმარებლო და სხვა სერვერები.

მონაცემი – ელექტრონული ფორმით წარმოდგენილი: ფაქტები, ცნებები, რიცხვები და სხვა, რომლთა დამუშავება ხდება კომპიუტერული და სხვა ელექტრონული მოწყობილობების დახმარებით;

მონაცემთა მესაკუთრე – სამსახურის/ფაკულტეტის/დეპარტამენტის ყველაზე მაღალი თანამდებობის პირი. გამონაკლის შემთხვევაში მონაცენთა მესაკუთრე შეიძლება იყოს სხვა პიროვნებაც;

მონაცემთა დამუშავება – მონაცემებზე ჩატარებული მოქმედებები: შექმნა, მიღება, ჩაწერა, შენახვა, შეგროვება, ორგანიზება, შეცვლა, წაკითხვა, ამოღება, გამოყენება, განთავსება, კომპოზიცია, წაშლა, განადგურება;

კომპიუტერული ანგარიში – სამუშაო სადგურის, ქსელის, ელფოსტისა და სასწავლო-საგამოცდო პროგრამების, ინტერნეტის გვერდების, სერვისებისა და პიროვნების განმსაზღვრელი ჩანაწერი.

მომხმარებელი – ნებისმიერი პიროვნება, რომელიც ამუშავებს უნივერსიტეტის მონაცემებს და აქვს კომპიუტერული ან ელფოსტის ანგარიში;

მომხმარებლის უფლება – კომპიუტერულ რესურსებთან წვდომის წესების ერთობლიობა, რომელიც განსაზღვრავს მონაცემებზე ჩასატარებელი მოქმედებებს: წაკითხვა, ჩაწერა, შესრულება, ცვლილება, ადმინისტრირება.

ავტორიზებული მომხმარებელი – უნივერსიტერის საზოგადოების წევრი ან ნებისმიერი პიროვნება, რომელიც აქვს კომპიუტერული ან ელფოსტის ანგარიში რითაც აქვს მინიჭებული უნივერსიტეტის მონაცემების დამუშავების უფლება;

ადმინისტრატორი მომხმარებელი – საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ განსაზღვრული უნივერსიტეტის საზოგადოების წევრები, რომელთაც ენიჭებათ კომპიუტერულ და საინფორმაციო რესურსებზე წვდომის განსაკუთრებული უფლებები (სისტემური ადმინისტრატორი, ადმინისტრატორი, მონაცემთა ბაზის ადმინისტრატორი, პროგრამული უზრუნველყოფის ადმინისტრატორი, აქტიური დირექტორიის ადმინისტრატორი და სხვა);

პირადი მონაცემი – პიროვნებასთან დაკავშირებული მონაცემი, რომლითაც ხდება მისი იდენტიფიცირება: დაბადების თარიღი, მისამართი, განათლებისა და შრომითი საქმიანობის ისტორია, ფინანსუსი საქმიანობა, ოჯახური მდგომარეობა და ა. შ.;

კონფიდენციალური პირადი მონაცემები – პიროვნებასთან დაკავშირებული რასობრივი თუ ეთნიკური წარმომავლობა, პოლიტიკური, რელიგიური, ფილოსოფიური შეხედულებები, ფიზიკური და გონებრივი ჯანმრთელობა, ნასამართლეობა და ა. შ.;

ინფორმაციის მთლიანიობა – ინფორმაციის დამუშავების, გადაცემის, ასახვის ან შენახვის დროს მისი იმ ფორმით შენარჩუნება, როგორც იყო შექმნილი. მონაცემთა სიზუსტისა და სრულყოფილების უზრუნველყოფა;

ინფორმაციისადმი წვდომა — ინფორმაციისადმი ხელმისაწვდომობის უზრუნველყოფა მომხმარებლის უფლების შესაბამისად;

ინფორმაციული უსაფრთხოება – ინფორმაციული რესურსებისა და სისტემების შემთხვევითი ან განზრახული დაზიანებისგან დაცვა, რომელმაც შეიძლება ზარალი მიაყენოს ინფორმაციის მესაკუთრეს ან მომხმარებელს;

ინფორმაციის დაცვა – ინფორმაციის მთლიანობის, კონფიდენციალურობისა და მიწვდომის პროცესის უზრუნველყოფის ორგანიზაციულ-ტექნიკური ღონისძიებათა კომპლექსი;

შემთხვევა/საფრთხე (ინციდენტი) – ინფორმაციული უსაფრთხოების დარღვევის, რეალური ან სავარაუდოდ შესაძლო შემთხვევა, რომელიც იწვევს მონაცემთა მთლიანობის, წვდომის ან კონფიდენციალურობის დარღვევას.

ქსელთაშორისი ეკრანი (Firewall) – კომპიუტერულ ქსელებს შორის წვდომის გამიჯვნის აპარატურულ-პროგრამული კომპლექსი;

კომპიუტერული ვირუსი და საზიანო პროგრამები – პროგრამების სახეობა, რომელთაც აქვთ უნარი შექმნან თავისი თავის ასლი, ჩაინერგონ სხვა პროგრამებში, ოპერატიულ მეხსიერებაში, დისკების ჩამტვირთველ ნაწილში, რომელთა მიზანია შეაფერხონ კომპიურეტული და ქსელური სისტემების მუშაობა, წაშალონ ფაილები, დაარღვიონ ფაილური სისტემები, დაარღვიოს მონაცემთა მთლიანობა და ა.შ.

საერთო მოხმარების კომპიუტერული რესურსები – კომპიუტერული რესურსები, რომელთა გამოყენებისათვის არაა საჭირო მომხმარებლის ავტორიზაცია;

ინტერნეტის განაწესი – (Internet Protocol – IP) კომპიუტერულ ქსელში მონაცემთა გადაცემის განაწესი.

ინტერნეტმისამართი – (IP მისამართი) კომპიუტერულ ქსელში არსებული მოწყობილობისთვის მინიჭებული რიცხვითი სიდიდე.

ელექტრონული ფოსტა – კომპიუტერულ ქსელში წერილების მიღებისა და გაგზავნის ტექნოლოგია.

კომპიუტერული კვანძების დინამიკურად მოწყობის განაწესი – (Dynamic Host Configuration Protocol – DHCP) არის ქსელის განაწესი, რომელიც გამოიყენება ინტერნეტის განაწესის (IP) მხარდაჭერის მქონე მოწყობილობებისათვის.

ოპერაციული სისტემა – კომპიუტერული პროგრამა, რომელიც მართავს კომპიუტერის აპარატურულ რესურსებსა და პროგრამულ უზრუნველყოფას.

სერვერული ოპერაციული სისტემა – ოპერაციული სისტემა, რომელიც მართავს სერვერულ კომპიუტერებს.

მარშრუტიზატორი – ქსელური მოწყობილობა/პროგრამა, რომლითაც ხდება სხვადასხვა ქსელში არსებულ მოწყობილობებს შორის მონაცემთა ურთიერთგაცვლა.

შესავალი

უნივერსიტეტის სასწავლო-სამეცნიერო მისიის შესრულებისათვის აუცილებელია, რომ თანამედროვე საინფორმაციო ტექნოლოგიების, კომპიუტერული სისტემებისა და პროგრამების, შიდა და გარე ქსელური მონაცემების, ინტერნეტის გამოყენება, მისაწვდომი გახდეს უნივერსიტეტის საზოგადოების წევრებისათვის.

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და პროცედურები წარმოადგენს უნივერსიტეტისა და მის დაქვემდებარებაში მყოფი კომპიუტერული და საინფორმაციო რესურსების გამოყენების განაწესების ერთობლიობას, რომლითაც უზრუნველყოფილ იქნება მომხმარებლის უფლება-მოვალეობების დაცვა, უნივერსიტეტის ელექტრონული მონაცემთა კლასიფიკაცია და ინფორმაციული უსაფრთხოება.

კომპიუტერული რესურსებისა და ქსელის გამოყენება

პოლიტიკის მიზანი

უნივერსიტეტის სასწავლო-სამეცნიერო მისიის შესრულებისათვის აუცილებელია თანამედროვე საინფორმაციო ტექნოლოგიების, კომპიუტერული სისტემებისა და პროგრამების, შიდა და გარე ქსელური მონაცემების, ინტერნეტის გამოყენება მისაწვდომი გახდეს უნივერსიტეტის საზოგადოების წევრებისათვის.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერულ, ქსელურ და საინფორმაციო რესურსებს. ასევე ყველა პიროვნება, რომელიც საკუთარ კომპიუტერს იყენებს უნივერსიტეტის კომპიუტერული რესურსებზე წვდომისათვის.

ზოგადი დებულებები

უნივერსიტეტის საკუთრებაში მყოფი და გამოყენებული საინფორმაციო რესურსები უნდა იყოს უნივერსიტეტის მისიისა და ღირებულებების შესაბამისი.

უნივერსიტეტის მფლობელობაში ან მისი ზედამხედველობის ქვეშ მყოფ კომპიუტერულ ტექნიკაზე დაყენებულია შეძენილი და/ან ლიცენზირებული ოპერაციული სისტემები, საოფისე პროგრამული პაკეტები, სამომხმარებლო გამოყენებითი პროგრამები, მონაცემთა ბაზების მართვის სისტემები, ინტერნეტში და ლოკალურ ქსელში სამუშაოდ საჭირო ქსელური მომსახურე პროგრამები, რომლებიც აუცილებელია უნივერსიტეტის ყოველდღიური საქმიანობისათვის.

უნივერსიტეტის კომპიუტერული ქსელისა ან რესურსების გამოყენება დასაშვებია მხოლოდ ავტორიზებული მომხმარებლისათვის. მომხმარებელი იყენებს კომპიუტერულ რესურსებს თავისი ანგარიშის უფლებამოსილების თანახმად(იხ. „მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა“),

უნივერსიტეტი, რომელიც ჩვეულებრივ არ ახდენს კომპიუტერულ ქსელში გადაცემული მასალის შემოწმებას ან შეზღუდვას, მაინც იტოვებს უფლებას, მოახდინოს ინდივიდუალური იდენტიფიცირების სესიების, ანგარიშის ფაილების, სისტემური პრობლემების, ვირუსებისა და სხვა საზიანო პროგრამების მონიტორინგი და განსაზღვროს არღვევს თუ არა მომხმარებელი საინფორმაციო რესურსების გამოყენების წესებს. უნივერსიტეტი ასევე იტოვებს

უფლებას მიახდინოს არასაუნივერსიტეტო კომპიუტერების მონიტორინგი, თუ ისინი უკავშირდება მის კომპიუტერულ რესურსებს.

უნივერსიტეტი, კომპიუტერული რესურსების გამოყენების წესების დარღვევის შემთხვევაში იტოვებს უფლებას შეუზღუდოს დამრღვევ მომხმარებელს უნივერსიტეტის საინფორმაციო რესურსებთან მიწვდომის უფლება.

მომხმარებლის პირადი კომპიუტერი, წესების დარღვევის შემთხვევაში, გაფრთხილების გარეშე გაითიშება უნივერსიტეტის კომპიუტერული ქსელიდან.

სახელმძღვანელო მითითებები

მომხმარებლის მოვალეობები

უნივერსიტეტის კომპიუტერული რესურსი უნივერისტეტის საზოგადოების წევრს (თანამშრომელს) მისი უნივერსიტეტში მუშაობის პერიოდში ეძლევა დროებით სარგებლობაში;

უნივერსიტეტის თანამშრომელი ვალდებულია მოვლილ და მუშა მდგომარეობაში იქონიოს მასზე დროებით გაპიროვნებული კომპიუტერული ტექნიკა, არ გაიტანოს იგი ადმინისტარციის ნებართვის გარეშე უნივერსიტეტის ტერიტორიიდან და არ გადასცეს გარეშე პირს. ტექნიკის უწესრიგობის აღმოჩენის შემთხვევაში თანამშრომელი ვალდებულია დროულად შეატყობინოს ამის შესახებ მის უშუალო ხელმძღვანელს, რომელიც თავის მხრივ წერილობით მიმართავს საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურს;

მომხმარებელი ვალდებულია დაიცვას და არ გადასცეს უნივერსიტეტის ხელმძღვანელობის თანხმობის გარეშე მესამე პირებს მონაცემები, რომელიც წარმოადგენს უნივერსიტეტისათვის კონფიდენციალურ ინფორმაციას (იხ. „მონაცემთა კლასიფიკაცია“) და ინახება უნივერსიტეტის კომპიუტერულ რესურსებზე.

ნებისმიერი სახის ოპერაციული სისტემის და/ან პროგრამული უზრუნველყოფის წაშლა/დაყენება, კონფიგურირება და გამართვა უნივერისტეტის კომპიუტერულ რესურსებზე (სამუშაო სადგურებზე, მობილურ კომპიუტერებზე და სხვა სახის პროგრამირებად ელექტრონულ მოწყობილობებზე) ხდება საინფორმაციო ტექნოლოგიების სამსახურის მიერ ან განსაკუთრებულ შემთხვევებში, უნივერსიტეტის მიერ მოწვეული კვალიფიცირებული სპეციალისტის მიერ.

უნივერსიტეტის საზოგადოების წევრი ვალდებულია გამოიყენოს უნივერსიტეტის მფლობელობაში ან ზედამხედველობის ქვეშ არსებული პროგრამული უზრუნველყოფა მხოლოდ კანონიერი მიზნებით, რომლებიც არ ეწინააღმდეგებიან საქართველოს კანონმდებლობასა და უნივერსიტეტის წესდებას.

მომხმარებელმა შეიძლება შეზღუდოს კომპიუტერული რესურსის გამოყენების უფლება. რესურსი შეზღუდულიც თუ არ იქნება, სხვა მომხმარებელს მაინც არ შეუძლია მესაკუთრის უფლების გარეშე: დაათვალიეროს, შექმნას ასლი, შეცვალოს ან წაშალოს სხვა მომხმარებლის ელექტრონული ფაილები. თუ რომელიმე მომხმარებელმა არ დახურა სამუშაო არე (სესია), მაშინ სხვა მომხმარებელი ვალდებულია დახუროს იგი. არაადმინისტრატორ მომხმარებლებს ეკრძალებათ აწარმოონ რომელიმე საინფორმაციო რესურსის მონიტორინგი ნებისმიერი მიზეზით.

მომხმარებლის მიერ კომპიუტერული რესურსების გამოყენება დაცულია საავტორო უფლებების კანონით[1] (იხ. ინფორმაციული ტექნოლოგიების რესურსების საავტორო უფლებები).

უნივერსიტეტის კომპუტერული და ქსელური რესურსები არ შეიძლება გამოყენებულ იქნეს რომელიმე პიროვნების ცილისწამებისა და შეურაცხყოფის მიზნით.

სტუდენტის მიერ სასწავლო/მასწავლი ტექნოლოგიები, შეტყობინებისა და ბლოგების პროგრამები არ შეიძლება გამოყენებულ იქნეს არაპატიოსანი გზით სასწავლო პროცესში აკადემიური შეფასების მისაღებად.

მომხმარებელმა არ უნდა მოახდინოს პროგრამული უზრუნველყოფის პარამეტრების ცვლილება ნებისმიერ კომპიუტერულ რესურსზე.

კომპიუტერული ანგარიშები, პაროლები და სხვა პირადი მონაცემები განკუთვნილია ინდივიდულური მომხმარებლებისთვის და დაუშვებელია მისი გაზიარება სხვა მომხმარებლისათვის (განსაკუთრებული შემთხვევების გარდა). მომხმარებელი პასუხისმგებელია საკუთარი ანგარიშის გამოყენებაზე (იხ. „მომხმარებლის ანგარიშის შექმნა და გაუქმება“). ავტორიზირებული სესიის დროს განხორციელებულ ყველა მოქმედებაზე პასუხისმგებელია ანგარიშის მფლობელი.

მომხმარებლმა არ უნდა შეასრულონ სამომხმარებლო პროგრამები ან/და შეცვალოს პროგრამული თუ აპარატურული უზრუნველყოფის პარამეტრები უნივერსიტეტის წვდომის კომპიუტერულ რესურსებზე.

მომხმარებლს ეკრძალება გამოიყენოს კომპიუტერული სისტემის მონაცემთა დაცვის გვერდის ავლის რაიმე ქმედებები. მაგ., გამოიყენონ ისეთი პროგრამები და სისტემები, რომლებიც მოახდენს პაროლების გამოცნობას.

აკრძალულია უნივერსიტეტის კომპიუტერული რესურსების ბოროტი განზრახვით გამოყენება. მაგალითად ისეთი ქმედებები როგორიცაა:

- მომხმარებელმა განზრახ არ უნდა გაავრცელოს ზიანის მომტანი პროგრამები: ვირუსები, ჭიები და სხვა;
- არ უნდა დააყენონ რაიმე პროგრამა საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის გარეშე;
- არ უნდა მოახდინონ კომპიუტერული პორტების სკანირება;
- არ უნდა მოახდინონ ქსელური ნაკადის გადატვირთვა, შეფერხება ქსელის გამოყენების დროს;
- მომხმარებელმა არ უნდა შეასრულოს ისეთი პროგრამები, რომლებიც არ არის დაშვებული რაიმე ამოცანის სასწავლო/კვლევითი ან მოდელირების მიზნებისათვის;
- მომხმარებელმა არ უნდა გამოიყენის ელექტრონული ფოსტა ე. წ. ჯაჭვური წერილების გასაგზავნად;
- აკრძალულია უნივერსიტეტის კომპიუტერული რესურსების გამოყენება გართობის მიზნით (თამაში, „ჭორაობა“ ან ინტერნეტგვერდების დათვალიერება და სხვა);
- არ უნდა მოახდინოს ელექტრონული კომუნიკაციების არაავტორიზებული მონიტორინგი;
- არ უნდა გამოიყენოს უნივერსიტეტის კომპიუტერული სისტემები პირადი კომერციული და ფინანსური მოგების მიღების მიზნით.

[1] მუხლები 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

მონაცემთა დაცვა

უნივერსიტეტი უზრუნველყოფს ცენტრალიზებულად შენახული ფაილების უსაფრთხოებას, დაარქივებას, სარეზერვო ასლების შექმნას უნივერსიტეტის საქმიანობის საჭიროებების საფუძველზე (გარდა მონაცემთა ურთიერთგაცვლისათვის შექმნილ საერთო საქაღალდეებისა).

უნივერსიტეტი პასუხს არ აგებს პირადი კომპიუტერის ან ნებისმიერი სხვა არაცენტრალიზებულად ან/და დაუცველად შენახული მომხმარებლების ფაილების ან მონაცემების დაცვაზე. მომხმარებელმა თვით უნდა დაიცვას თავისი ინფორმაცია: მოახდინოს მნიშვნელოვანი ინფორმაციის სარეზერვო ასლების შექმნა და სათანადო დაცვა.

უნივერსიტეტის ყველა კომპიუტერულ სისტემაზე უნდა იყოს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ (რეკომენდირებული) დაყენებული ანტივირუსული პროგრამული უზრუნველყოფა.

უნივერსიტეტი ცდილობს უზრუნველყოს მისი მონაცემთა უსაფრთხოება, სარეზერვო ასლების შენახვა და მონაცემთა აღდგენა მისი შემთხვევითი დაზიანების დროს, მაგრამ არაა პასუხისმგებელი ელენერგიის, ხანძრის, წყალდიდობის, არაავტორიზებული წვდომის შედეგად დაზიანებულ ან დაკარგულ მონაცემებზე.

საფრთხის შესახებ შეტყობინება

უნივერსიტეტის გამოთვლითი რესურსების გამოყენების საფრთხე შეიძლება განისაზღვროს რაიმე მოქმედებით ან მოვლენით, რომელმაც შეიძლება ზიანი მიაყენოს მონაცემთა უსაფრთხოებას, მთლიანობასა ან კომპიუტერული რესურსების ხელმისაწვდომობას. საფრთხის შემთხვევის შესახებ მომხმარებელმა უნდა შეატყობინოს საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურს.

სანქციები

ინფორმაციული ტექნოლოგიების გამოყენების წესების დარღვევის დროს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური შეაჩერებს შესაბამისი სერვისების გამოყენებას, რაც გამოიხატება მომხმარებელთა უფლებების დროებით ან მუდმივ შეზღუდვა-შეჩერებაში და საჭიროების შემთხვევაში მიაწოდებს დარღვევის შესახებ ინფორმაციას უნივერსიტეტის ადმინისტრაციას.

მომხმარებლის ანგარიშის შექმნა და გაუქმება

პოლიტიკის მიზანი

მომხმარებლის ანგარიშის შექმნისა და გაუქმების პოლიტიკით განსაზღვრულია უნივერსიტეტის კომპიუტერულ რესურსებთან და ელფოსტასთან უნივერსიტეტის საზოგადოების წევრების იდენტიფიცირების განაწესი.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე

ზოგადი დებულებები

უნივერსიტეტის კომპიუტერული რესურსებისა და ელფოსტის გამოყენებისათვის არსებობს მომხმარებელთა ჩვეულებრივი და განსაკუთრებული უფლებების (იხ. „მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა“) მქონე ანგარიშები.

განსაკუთრებელი უფლებების მქონე (ადმინისტრატორი) მომხმარებელს განსაზღვრავს საინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის ხელმძღვანელი, ხოლო უნივერსიტეტის საზოგადოების ყველა დანარჩენ წევრს აქვს ჩვეულებრივი სამომხმარებლო ანგარიში

სახელმძღვანელო მითითებები

მომხმარებლის ანგარიშის შექმნა

ფაკულტეტის წევრები/თანამშრომლები: ადამიანური რესურსების მართვის სამსახურის მიერ მოწოდებული ახალ თანამშრომელთა სიის თანახმად საინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური ყოველი თანამშომლისათვის ქმნის კომპიუტერულ და ელფოსტის ანგარიშს. ფაკულტეტის სასწავლო-სამეცნიერო აკადემიური პერსონალისათვის ფაკულტეტის ხელმძღვანელის წარდგინებით იქმნება სასწავლო/მასწავლი პროგრამების ანგარიში.

სტუდენტები: ყოველი ახალი სტუდენტისათვის მისი რეგისტრაციისთანავე იქმნება ელფოსტისა და სასწავლო/მასწავლი პროგრამების ანგარიშები.

ანგარიშების გაუქმება

ფაკულტეტის წევრები/თანამშრომლები: ადამიანთა რესურსების სამსახურის მიერ გადმოცემული უნივერსიტეტიდან წასულ თანამშრომელთა სიის მიხედვით, ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური აუქმებს ამ თანამშრომელთა შესაბამის ანგარიშებს.

სტუდენტები: სტუდენტის სტატუსის ცვლილება გავლენას არ ახდენს ელფოსტის ანგარიშზე. უნივერსიტეტის დამთავრების ან სტატუსის შეწყვეტა/შეჩერების შემდეგ განისაზღვრება მისი ანგარიშით უნივერსიტეტის კომპიუტერულ რესურსებზე წვდომის შეზღუდული უფლებები.

პაროლის შექმნა და გამოყენება

პოლიტიკის მიზანი

პაროლის შექმნისა და გამოყენების პოლიტიკის მიზანია ჩამოაყალიბოს პაროლის შექმნის, გამოყენებისა და დაცვის წესები.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომელთაც აქვთ მომხმარებლის ანგარიში.

ზოგადი დებულებები

პაროლი ინფორმაციული და ქსელური უსაფრთხოების მნიშვნელოვანი კომპონენტია. მომხმარებლის სახელი და პაროლი ერთად ემსახურება მომხმარებლის ნამდვილობის შემოწმებას.

მომხმარებლის მიერ ყველა სახის ანგარიშის პაროლის შექმნა, გამოყენება და დაცვა უნდა ემორჩილებოდეს ამ პოლიტიკას.

სახელმძღვანელო მითითებები

უნივერსიტეტში არსებობს სხვადასხვა სახის მომხმარებლის კომპიუტერული ანგარიშები (იხ. „მომხმარებლის ანგარიშის შექმნა და გაუქმება“). ადმინისტრატორი მომხმარებლის დონის ყველა ანგარიშის პაროლი უნდა შეიცვალოს ყოველი 60 დღის შემდეგ. ჩვეულებრივი მომხმარებლის დონის ანგარიშების (კომპიუტერული, ელფოსტის, სამომხმარებლო პროგრამული) პაროლები უნდა შეიცვალოს ყოველი 90 დღის შემდეგ.

პაროლი წარმოადგენს ტექსტურ სიდიდეს. ყოველი მომხმარებლი ანგარიშის შექმნისთანავე ღებულობს ადმინისტრატორისგან ერთჯერად პაროლს და ვალდებულია შეცვალოს იგი პირველივე გამოყენების დროს.

პაროლის შემქმნისთვის უნდა იქნეს გათვალისწინებული, რომ პაროლი:

1. უნდა შეიცავდეს ლათინური ანბანის დიდ და პატარა სიმბოლოებს (მაგ.: a-z, A-Z);
2. უნდა შეიცავდეს ციფრს, არითმეტიკული მოქმედების ან/და სხვა სიმბოლოებს (მაგ.: 0-9, @#$%^&*()_+|~- =\`{}[]:";'<>?,./);
3. სიგრძე (სიმბოლოთა რაოდენობა) უნდა იყოს არანაკლებ 8 ალფავიტურ-ციფრული სიმბოლო;
4. არ უნდა იყოს არც ერთი ბუნებრივი ენის რაიმე სიტყვა (პიროვნების გვარი და სახელი, შინაური ცხოველების, ქალაქებისა და სხვა სახელები, კომპიუტერული ტერმინები, ბრძანებები, დაწესებულებების სახელები და სხვა; დაბადების თარიღები, მისამართები, ტელეფონის ნომრები და სხვა; შემდეგი სახის სიტყვები: aaabbb, qwerty, zyxwvuts, password, 123321, secret1, 1secret და სხვა);
5. ადვილად რომ დავიმახსოვროთ, შეიძლება გამოვიყენოთ რაიმე ფრაზის აბრევიატურა.

პაროლის დაცვისთვის უნდა იქნეს გათვალისწინებული, რომ მომხმარებელმა:

1. არ უნდა გამოიყენოს ერთი და იგივე პაროლი უნივერსიტეტის ანგარიშებისა და სხვა ანგარიშებისათვის (მაგ., პირადი ელფოსტის ანგარიში);
2. არ უნდა გაუზიაროს უნივერსიტეტის ანგარიშების პაროლების სხვას, მათ შორის ადმინისტრაციის წარმომადგენლებს, მდივნებს, თანამშრომლებსა ან კოლეგებს (მაგ., შვებულებაში ყოფნის დროსაც კი), ოჯახის წევრებს. ყველა პაროლი არის პირადი ინფორმაცია;
3. არ დაწეროს ან შეინახოს პაროლი ელექტრული ფორმით;

4. არ გააგზავნოს პაროლი ელფოსტით ან ნებისმიერი სხვა კომუნიკაციური საშუალებით (მაგ., ტელეფონით);
5. არ ისაუბროს პაროლის შესახებ;
6. არ გაამჟღავნოს პაროლი პაროლის შეხსენებაში;
7. არ გამოიყენოს „დამიმახსოვრე“ პარამეტრი.

საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის თანამშრომელმა შეიძლება მოითხოვოს მომხმარებლის პაროლი მისი დახმარების მოთხოვნის შემთხვევაში.

პაროლის გამჟღავნების ეჭვის შემთხვევა მომხმარებელმა უნდა შეატყობინოს საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურს.

მომხმარებლის ანგარიშის წვდომის უფლება და შეზღუდვა

პოლიტიკის მიზანი

მომხმარებლის ანგარიშის წვდომის უფლებისა და შეზღუდვის პოლიტიკა განსაზღვრავს უნივერსიტეტის კომპიუტერილი რესურების არაავტორიზებული ან/და არადანიშნულებით გამოყენებისაგან დაცვის წესებს.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომელთაც აქვთ უნივერსიტეტის კომპიუტერული რესურსებისა და ელფოსტის ანგარიში.

ზოგადი დებულებები

მომხმარებლის უფლება წარმოადგენს კომპიუტერულ რესურსებთან წვდომის წესების ერთობლიობას, რომელიც განსაზღვრავს მონაცემებზე ჩასატარებელი მოქმედებებს: წაკითხვა, ჩაწერა, შესრულება, ცვლილება, ადმინისტრირება.

სახელმძღვანელო მითითებები

ინფორმაციული ტექნოლოგიების მიწვდომის უფლების მინიჭება: მომხმარებელს მხოლოდ იმ კონკრეტულ რესურსებთან მიწვდომის უფლება ენიჭება, რომლებიც საჭიროა მისი უშუალო სამსახურეობრივი/აკადემიური მოვალეობების შესასრულებლად. უფლებები განისაზღვრება (იცვლება ან/და უქმდება) მისი დეპარტამენტის (სამსახურის) ხელმძღვანელის მიერ. მომხმარებლებს ეკრძალებათ საერთო მოხმარების რესურსების გარდა სხვა კომპიუტერული რესურსის გამოყენება ავტორიზაციის გარეშე.

წვდომის უფლებათა ცვლილება: თუ მომხმარებელი შეიცვლის თანამდებობას ან/და პასუხისმგებლობას უნივერსიტეტში, მომხმარებლის წვდომის უფლებები უნდა გადაიხედოს. მომხმარებელმა უნდა გამოიყენოს კომპიუტერული რესურსების მხოლოდ ის ობიექტები, ანგარიშები, წვდომის კოდები, პრივილეგიები ან/და ინფორმაცია, რომლისთვისაც არის უფლებამოსილი მისი ახალი თანამდებობის პასუხისმგებლობის მიხედვით.

ანგარიშის წვდომის გაზიარება: არ შეიძლება მომხმარებელმა თავისი ანგარიშები, პაროლები გაუზიაროს სხვებს. მომხმარებელი პასუხისმგებელია თავისი ანგარიშით ჩატარებულ მოქმედებებზე. უნივერსიტეტის დაქვემდებარებაში არსებული კომპიუტერის საშუალებით განხორციელებული ნებისმიერი ქმედებისათვის პასუხისმგებლობა ეკისრებათ მომხმარებლებს.

უნივერსიტეტის ელექტრონული ფოსტა

პოლიტიკის მიზანი

უნივერსიტეტის ელექტრონული ფოსტის პოლიტიკა განსაზღვრავს ელექტრონული ფოსტის მართვის წესებს.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომელთაც აქვთ უნივერსიტეტის ელფოსტის ანგარიში.

ზოგადი დებულებები

ელექტრონული ფოსტა არის უნივერსიტეტის საზოგადოების წევრებისათვის ერთ-ერთი მნიშვნელოვანი შიდა და გარე კომუნიკაციის საშუალება. ელექტრონული ფოსტა, რომელიც ფუნქციონირებს @atsu.edu.ge დომენით, წარმოადგენს უნივერსიტეტის საკუთრებასა და შეიძლება გამოყენებულ იქნეს, მხოლოდ სამსახურებრივი მიზნებით. წერილის შინაარსის არწაკითხვა, არმიღება ან წაშლა არ ათავისუფლებს პასუხისმგებლობისაგან ელფოსტის ანგარიშის მფლობელს.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის[2] თანახმად უნივერსიტეტის თანამშრომლებისა და სტუდენტების ელექტრონული ფოსტის ინდივიდუალური ანგარიშიდან განხორციელებული მიმოწერა წარმოადგენს მათ პირად ინფორმაციას და არ ექვემდებარება შინაარსობრივ მონიტორინგს, კანონმდებლობით განსაზღვრული შემთხვევების გარდა.

ელექტრონული ფოსტის სისტემის მუშაობასთან დაკავშირებული ნებისმიერი კითხვით უნივერსიტეტის საზოგადოების წევრებმა უნდა მიმართოს თავის უშუალო ხელმძღვანელსა და/ან უნივერსიტეტის ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურს.

სახელმძღვანელო მითითებები

ელექტრონული ფოსტის გამოყენება

ელფოსტის გამოყენების სახეები მოიცავს, მაგრამ არ შემოიფარგლება:

- უნივერსიტეტის საზოგადოების წევრებსა ან/და უნივერსიტეტის საქმიან პარტნიორებთან პირადი პასუხისმგებლობით კომუნიკაცია, ინფორმაციის გაცნობა/გაზიარება;
- საგანმანათლებლო, კვლევითი ან/და პროფესიული განვითარების საქმიანობაში მონაწილეობა.

დაუშვებელია:

- საავტორო უფლებების დარღვევა, უხამსობის, შეურაცხყოფისა და ცილისწამების გავრცელება, თაღლითობა, პლაგიატი, დაშინება, გაყალბება, უკანონო პირამიდული სქემების შექმნა ან კომპიუტერული საზიანო პროგრამების გავრცელება და სხვა;
- ელფოსტის ანგარიშების ან ფაილების დათვალიერება, ასლის შექმნა, შეცვლა ან წაშლა ამ ანგარიშის მფლობელის ან სხვა პირის ნებართვის გარეშე;

[2] საქართველოს კანონი „**პერსონალურ მონაცემთა დაცვის შესახებ**“ – **https://matsne.gov.ge/ka/document/view/1561437**

- ელფოსტის საეჭვო მისამართებიდან გამოგზავნილი შეტყობინების თანდართული დოკუმენტების, რომლებიც არიან ვირუსებისა და საზიანო პროგრამების გავრცელების პირდაპირი წყაროები, გახსნა;
- ელფოსტის ანგარიშის პაროლების გაზიარება სხვა პიროვნებასათვის ან სხვა პირის ელფოსტის ანგარიშის პაროლის გაგების მცდელობა;
- ელფოსტის კომერციული საქმიანობის, პოლიტიკური კამპანიის, ჯაჭვური წერილების გავრცელებისა და სხვა ასეთი საქმიანობისთვის გამოყენება.

ელექტრონული ფოსტის ანგარიშის შექმნა

უნივერსიტეტში გამოიყენება შემდეგი ტიპის ელექტრონულ ფოსტის ანგარიში (იხ. პოლიტიკა „მომხმარებლის ანგარიშის შექმნა და გაუქმება“):

- უნივერსიტეტის თანამშრომლებისა და სტუდენტების ინდივიდუალური ანგარიში. ანგარიში ფორმირდება სახელისა და გვარის კომბინაციით, იმ შემთხვევაში თუ აღნიშნული კომბინაცია დაკავებულია, ემატება რიგითი ნომერი (დარეგისტრირების თანმიმდევრობის მიხედვით);
- ცალკეული სტრუქტურული ერთეულის (ფაკულტეტი, დეპარტამენტი და ა. შ.), კვლევით, სამეცნიერო, კულტურულ და სოციალური პროექტების და სხვა სპეციალური საფოსტო ანგარიშები ფორმირდება შესაბამის სამსახურებთან შეთანხმებით და მათი მიმართვის საფუძველზე;

ელექტრონული ფოსტის ანგარიშის შეჩერება/გაუქმება

ელექტრონული ფოსტის ანგარიშის ფუნქციონირების შეჩერება ხდება შემდეგ შემთხვევებში:

- უნივერსიტეტის საზოგადოების მიერ “კომპიუტერული რესურსებისა და ქსელის გამოყენება” პოლიტიკის დარღვევა;
- თანამშრომლისათვის მისი უნივერიტეტიდან გათავისუფლება;
- სტუდენტისათვის სტატუსის შეწყვეტა ან სხვა უნივერსიტეტში გადასვლა;
- ცალკეული სტრუქტურული ერთეულის ლიკვიდაცია/რეორგანიზაცია.
- უნივერსიტეტის ელექტრონული ფოსტის არამიზნობრივი გამოყენება;
- ამ პოლიტიკითა და საქართველოს კანონმდებლობით აკრძალული ინფორმაციის გავრცელება;
- მესამე პირის მიერ ანგარიშზე წვდომის გამოვლენა.

უნივერსიტეტის ელექტრონული ფოსტის ანგარიშის ფუნქციონირების დროებითი შეჩერების შემთხვევაში ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური ვალდებულია შეატყობინოს ამ ფაქტის შესახებ, როგორც ანგარიშის მფლობელს, ასევე მისი უშუალო ხელმძღვანელს;

შეზღუდვა იხსნება მისი გამომწვევი მიზეზების აღმოფხვრის შემდეგ და ამის შესახებ ეცნობება, როგორც ანგარიშის მფლობელს, ასევე მის უშუალო ხელმძღვანელს.

მონიტორინგი

უნივერსიტეტის ადმინისტრაციის ნებართვით, ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურმა შეიძლება მონიტორინგი გაუწიოს ნებისმიერ ოფიციალურ კომუნიკაციას, მათ შორის ელფოსტას, თუ არსებობს უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ბოროტად გამოყენების ან დარღვევის საფუძვლიანი ეჭვი.

სამსახურს შეუძლია დაათვალიეროს მომხმარებლის ელფოსტა შემდეგ შემთხვევებში:

ა) საუნივერსიტეტო საქმიანობის უწყვეტობის უზრუნველყოფისათვის (მაგ., ინფორმაციის მიღების საჭიროების შემთხვევაში მაშინ, როცა მომხმარებელი მიუწვდომელია);

ბ) სისტემასთან დაკავშირებული ტექნიკური პრობლემების დიაგნოსტიკისა და აღმოფხვრისათვის;

გ) გამოიძიოს ელფოსტის შესაძლო არასათანადო გამოყენება, როდესაც არსებობს ბოროტად გამოყენების საფუძვლიანი ეჭვი ან დამტკიცებულია გამოძიებით.

მონაცემთა კლასიფიკაცია

პოლიტიკის მიზანი

მონაცემთა კლასიფიკაციის პოლიტიკის მიზანია მონაცემთა მესაკუთრეთა მოთხოვნის შესაბამისად უნივერსიტეტის მონაცემების დახარისხება მისი კონფიდენციალობის, ღირებულებისა და კრიტიკულობის დონის მიხედვით. მონაცემთა კლასიფიკაციით განსაზღვრულია მონაცემების დაცვის საბაზისო წესები.

გავრცელების არე

ეს პოლიტიკა ვრცელდება მხოლოდ ელექტრუნულ მონაცემებზე და ეხება მონაცემთა მესაკუთრეებს, უნივერსიტეტის საზოგადოების წევრებს, რომლებიც უფლებამოსილნი არიან გამოიყენონ უნივერსიტეტის მონაცემები და საინფორმაციო რესურსები.

ზოგადი დებულებები

ინფორმაციული უსაფრთხოების მიხედვით მონაცემთა კლასიფიკაცია ხორციელდება მისი კონფიდენციალობისა და უნივერსიტეტის საქმიანობაზე გავლენის დონის მიხედვით. მონაცემების კლასიფიკაცია არ უნდა ზღუდავდეს მონაცემებს ზედმეტად. უნივერსიტეტის ყველა მონაცემი უნდა იყოს კლასიფიცირებული კონფიდენციალობის სამი შემდეგი დონის მიხედვით:

შეზღუდული მონაცემები: მონაცემები კლასიფიცირებულია როგორც შეზღუდული, მაშინ როცა მონაცემთა არასანქცირებულმა გამჟღავნებამ, შეცვლამ ან განადგურებამ შეიძლება გამოიწვიოს უნივერსიტეტის საქმიანობისათვის საფრთხის რისკის მაღალი დონე. შეზღუდული მონაცემები დაცულია სახელმწიფო კანონმდებლობით და კონფიდენციალურობის შეთანხმებებით (მაგ., სტუდენტთა აკადემიური მონაცემები, ექსტრანეტი, ფინანსური ინფორმაცია და სხვა). უსაფრთხოების ყველაზე მაღალი დონე უნდა იქნეს გამოყენებული შეზღუდული მონაცემებისათვის.

პირადი მონაცემები: მონაცემები კლასიფიცირებულია როგორც კერძო, პირადი (სამედიცინო ჩანაწერები, სტუდენთა აკადემიური ჩანაწერები, საბანკო ან პირადი ფინანსური ინფორმაცია), მაშინ როცა, მონაცემთა არასანქცირებულმა გამჟღავნებამ, შეცვლამ ან განადგურებამ შეიძლება გამოიწვიოს უნივერსიტეტის საქმიანობისათვის საფრთხის რისკის საშუალო დონე. ჩვეულებრივ, უნივერსიტეტის ყველა მონაცემი, რომელიც არ არის აშკარად კლასიფიცირებული, როგორც **შეზღუდული** ან **საჯარო** მონაცემი უნდა მიკუთვნოს **პირად მონაცემებს**. პირადი მონაცემების დაცვა უნდა მოხდეს უსაფრთხოების საშუალო დონის მიხედვით.

საჯარო მონაცემები: მონაცემები კლასიფიცირებულია, როგორც საჯარო მაშინ, როცა მონაცემთა არასანქცირებულმა გამჟღავნებამ, შეცვლამ ან განადგურებამ შეიძლება არ გამოიწვიოს ან გამოიწვიოს უნივერსიტეტის საქმიანობისათვის მცირე საფრთხის რისკი. საჯარო მონაცემების მაგალითებია: განცხადებები, შეტყობინებები, კურსის სასწავლო განრიგი, პრესრელიზები, საინფორმაციო ბიულეტენი, გაზეთები, ჟურნალები, ვებ-გვერდები, სამეცნიერო ნაშრომები და სხვა. საჯარო მონაცემების დაცვისათვის საჭიროა უსაფრთხოების დაბალი დონე.

უსაფრთხოების საშუალო ან მაღალი დონე საჭიროა მონაცემების არასანქცირებული მოდიფიცირების ან განადგურების თავიდან აცილების მიზნით. საჯარო მონაცემები განკუთვნილია როგორც უნივერსიტეტის საზოგადიების წევრის, ისე სხვა ნებისმიერი მომხმარებლისათვის.

მონაცემთა დაცვა

პოლიტიკის მიზანი

მონაცემთა დაცვის პოლიტიკის მიზანია უნივერსიტეტის საინფორმაციო რესურსებისა და სისტემების მონაცემთა შენახვის, დაამუშავებისა და გადაცემის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის საინფორმაციო რესურსებს და სისტემებს.

ზოგადი დებულებები

უნივერსიტეტის ყველა მონაცემი და ინფორმაციული სისტემა, დაცული უნდა იქნეს შესაბამისად კონფიდენციალურობის, ღირებულებისა და აუცილებლობის დონის გათვალისწინებით..

სახელმძღვანელო მითითებები

უნივერსიტეტის საინფორმაციო რესურსებთან მიწვდომა განისაზღვრება მომხმარებლის უფლებებით (იხ. „მომხმარებლის წვდომის უფლება და შეზღუდვა“).

მომხმარებელმა უნდა დაიცვას არა მხოლოდ უნივერსიტეტის, არამედ სხვა მომხმარებლებისა და მესამე პირების მიერ დაწესებული შეზღუდვები, რომლებიც არ ეწინააღმდეგება უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას.

საავტორო უფლებები

პოლიტიკის მიზანი

საავტორო უფლებების პოლიტიკის მიზანია: პროგრამული უზრუნველყოფის, მონაცემთა ბაზების და სხვა ელექტრონული ფორმატით წარმოდგენილი ნამუშევრების (ლიტერატურული, მუსიკალური თუ მხატვრული ნაწარმოებების, ფოტოსურათების, კინო-ფილმების, ვიდეოჩანაწერებისა და სხვა), რომლებიც დაცულია „საავტორო უფლებებით“, შემქმნელთა ინტელექტუალური საკუთრების უფლების დაცვა და საავტორო უფლებების დარღვევასთან დაკავშირებული პრობლემების თავიდან აცილება.

გავრცელების არე

ეს პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერულ ქსელსა და რესურსებს.

ზოგადი დებულებები

უნივერსიტეტის მფლობელობაში ან მისი ზედამხედველობის ქვეშ მყოფ კომპიუტერულ ტექნიკაზე დაყენებულია შეძენილი და/ან ლიცენზირებული ოპერაციული სისტემები, საოფისე პროგრამული პაკეტები, სამომხმარებლო გამოყენებითი პროგრამები, მონაცემთა ბაზების მართვის სისტემები, ინტერნეტში და ლოკალურ ქსელში სამუშაოდ საჭირო ქსელური მომსახურე პროგრამები, რომლებიც აუცილებელია უნივერსიტეტის ყოველდღიური საქმიანობისათვის.

უნივერსიტეტი იზიარებს საქართველოს კანონის მოთხოვნებს საავტორო და მომიჯნავე უფლებების შესახებ[3]. უნივერსიტეტის კომპიუტერულ ქსელში არსებული პროგრამული უზრუნველყოფა და მონაცემთა ბაზები ეკუთვნის ან ლიცენზირებულია უნივერსიტეტის ან მესამე მხარის მიერ და დაცულია საავტორო უფლებებით, ლიცენზირებისა და ხელშეკრულებათა წესებითა და სხვა კანონებით. მომხმარებელი ვალდებულია პატივი სცეს და დაიცვას პროგრამული უზრუნველყოფის გამოყენებისა და განაწილების ლიცენზიების პირობები, რომელიც შეიცავს შემდეგი სახის აკრძალვას:

1. უნივერსიტეტის ქსელში გამოყენების მიზნით პროგრამების ასლის შექმნა ან უნივერსიტეტის ფარგლებს გარეთ მისი გავრცელება;
2. საავტორო უფლებებით დაცული ნამუშევრების არასანქცირებული ჩამოტვირთვა და საუნივერსიტეტო კომპიუტერულ ქსელში ან/და სხვა საინფორმაციო რესურსების საშუალებით გამოყენება;
3. მონაცემთა ან/და პროგრამების გაყიდვა;
4. პროგრამული უზრუნველყოფის გამოყენება არასასწავლო მიზნებისა ან/და ფინანსური მოგებისათვის;
5. პროგრამების (მაგ.: პროგრამული კოდის) ან მონაცემების მათი ავტორების / მფლობელების ნებართვის გარეშე საჯაროდ გამჟღავნება.

უნივერსიტეტის ქსელთან დაკავშირებისას ყველა მომხმარებელი ვალდებულია დაიცვას ნამუშევრების საავტორო უფლებები, რომლებიც ხელშეკრულების შეთანხმების სახით ჩვეულებრივ განთავსებულია მომწოდებლის ვებგვერდზე. მომხმარებელი რომ არ დაეთანხმოს კონკრეტულ საავტორო უფლებებს, ეს მაინც არ ნიშნავს, რომ საავტორო უფლებები არ ვრცელდება ამ ნამუშევარზე.

[3] მუხლები 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

სანქციები

პოლიტიკის მიზანი

სანქციების პოლიტიკა აღწერს უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკისა ~~ან/და ნებისმიერ მოქმედი კანონმდებლობის~~ დარღვევის შემთხვევაში უნივერსიტეტის საზოგადოების წევრებზე გატარებულ მოქმედებებს/სანქციებს.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერულ ქსელსა ან/და რესურსებს.

ზოგადი დებულებები

ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დარღვევის დროს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ ხდება ინფორმაციული სერვისების დაუყოვნებლივ შეჩერება, რომელიც შეიძლება მოიცავდეს მომხმარებელთა უფლებების (იხ. „მომხმარებელთა უფლებები და შეზღუდვა“) დროებით შეჩერებას ან გაუქმებასა და საჭიროების შემთხვევაში მიაწოდებს დარღვევის შესახებ ინფორმაციას უნივერსიტეტის ადმინისტრაციას.

ვირუსებისა და საზიანო პროგრამებისგან დაცვა

პოლიტიკის მიზანი

ვირუსებისა და საზიანო პროგრამებისგან დაცვის პოლიტიკის მიზანია კომპიუტერული ვირუსების და სხვა საზიანო პროგრამების (ჭიები, ტროიანული ცხენები და ა.შ) გავრცელების თავიდან აცილება.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერულ ქსელსა ან/და რესურსებს.

ზოგადი დებულებები

ვირუსები და საზიანო პროგრამები, რომლებიც შექმნილია ელექტრონული ინფორმაციის დაზიანების, მოპარვის, მოდიფიცირებისა და სხვა საზიანო ქმედებისათვის, საფრთხეს უქმნის უნივერსიტეტის ინფორმციულ უსაფრთხოებას.

სახელმძღვანელო მითითებები

უნივერსიტეტის ყველა სამუშაო სადგურზე, კომპიუტერზე, ფაილურ- თუ ვებ-სერვერზე, ელექტრონული ფოსტის სისტემაში, რომლებიც დაკავშირებულია უნივერსიტეტის კომპიუტერულ ქსელთან, უნდა დაყენდეს, საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ რეკომენდირებული ვირუსებისა და საზიანო პროგრამებისაგან დაცვის პროგრამული უზრუნველყოფა და შესაბამისი პარამეტრები, მოხდეს ვირუსების გამოვლენა და განადგურება.

ვირუსებისა და საზიანო პროგრამებისაგან დაცვის პროგრამული უზრუნველყოფა არ უნდა იყოს გამორთული. მისი პარამეტრები არ უნდა შეიცვალოს ისე, რომ შეამციროს დაცვის ეფექტურობა. არ უნდა შეიცვალოს ამ პროგრამების მონაცემთა ბაზის ავტომატური განახლების სიხშირე, კერძოდ, არ უნდა შემცირდეს.

ავტომატურად გამოვლენილი და განადგულებული ყველა ვირუსის შესახებ ინფორმაცია, როგორც ინფორმაციული საფრთხის შემთხვევა, უნდა ეცნობოს საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურს.

მობილური მოწყობილობების გამოყენება

პოლიტიკის მიზანი

მობილური მოწყობილობის გამოყენების პოლიტიკა განსაზღვრავს სმარტფონების, ტაბლეტკომპიუტერისა და სხვა მობილური მოწყობილობებით უნივერსიტიტის საინფორმაციო რესურსების გამოყენების განაწესს.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერულ ქსელს, ელექტრონულ ფოსტასა და რესურსებს მობილური ელექტრონულ მოწყობილობის საშუალებით.

ზოგადი დებულებები

მობილური მოწყობილობაა პატარა ზომის კომპიუტერი, რომლის გადაადგილება ადვილია და აქვს სამაგიდო კომპიუტერის მრავალი ფუნქცია.

სახელმძღვანელო მითითებები

მობილური მოწყობილობით უნივერსიტეტის კომპიუტერული რესურსების მონაცემების დამუშავების დროს საჭიროა, რომ:

- უნივერსიტეტის მონაცემების შესანახად გამოვიყენოთ მხოლოდ პაროლით დაცული მობილური მოწყობილობები;
- პაროლის ფორმირება და გამოყენება უნდა მოხდეს უნივერსიტეტის „პაროლის შექმნისა და გამოყენების“ პოლიტიკის შესაბამისად;
- დაკარგული, მოპარული ან გადაადგილებული მობილური მოწყობილობა უნდა იყოს გაცხადებული, როგორც შესაბამის ოპერატორთან, ისე უნივერსიტეტის საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურში;
- მომხმარებელი პასუხისმგებელია მობილური მოწყობილების გამოყენებაზე მაშინაც კი, თუ თავისი ნებით გადასცა ის მესამე პირს;
- მობილური მოწყობილობების უსადენო კავშირის სისტემა იყოს სათანადოდ კონფიგურირებული ან გამორთული;
- მობილური მოწყობილობის დაკარგვის, დაზიანებისა ან დამუხტვის ელემენტის მოქმედების დასრულების დროს გამოწვეული შეფერხების თავიდან ასაცილებლად რეგულარულად იქმნებოდეს მონაცემების სარეზერვო ასლი (იხ. “სარეზერვო ასლის შექმნა და მონაცემთა აღდგენის“ პოლიტიკა);
- მობილური მოწყობილობასა და კომპიუტერის მონაცემთა ურთიერთგაცვლის დროს მომხმარებელი დარწმუნდეს, რომ პერსონალურ კომპიუტერში არსებული შეზღუდული მონაცემები დაცულია;
- შეიცვალოს ელფოსტის პაროლი, თუ დაიკარგა მობილური მოწყობილობა, რომელიც გამოიყენება უნივერსიტეტის ელფოსტის წვდომისთვის.

გადასატანი მედიამოწყობილობების გამოყენება

პოლიტიკის მიზანი

გადასატანი მედიამოწყობილობების გამოყენების პოლიტიკის მიზანია ჩამოაყალიბოს უნივერსიტეტის კონფიდენციალური ინფორმაციის დაკარგვა/დაზიანების რისკის შემცირებისა და ვირუსისა და საზიანო პროგრამების გავრცელებისაგან კომპიუტერული ქსელის დაცვის განაწესი.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების წევრებზე, რომლებიც იყენებენ უნივერსიტეტის საინფორმაციო რესურსებს მათი ინფორმაციის: USB მოწყობილობებით, ოპტიკური დისკებით და ნებისმიერი სხვა ფიზიკური მედიამოწყობილობებით შენახვისა და გადატანისათვის.

ზოგადი დებულებები

გადასატანი მედიამოწყობილობები, რომელიც შეიძლება მიუერთდეს უნივერსიტეტის კომპიუტერულ რესურსებს შესაძლოა გამოყენებულ იქნეს ინფორმაციის შესანახად. ასეთ მოწყობილობებს განეკუთვნება: ციფრული კამერა, გარე დისკები და სხვა.

სახელმძღვანელო მითითებები

აუცილებელია გადასატანი მედიამოწყობილობა შემოწმდეს საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ რეკომენდირებული და დაყენებული ანტივირუსული პროგრამით. კონფედენციალური მონაცემების შემცველი მოწყობილობა ასევე ფიზიკურად უნდა იქნეს დაცული.

გადასატან მედიამოწყობილობასთან მუშაობის დასრულების დროს უნდა იქნეს გამოყენებული მისი პერსონალური კომპიუტერიდან გამორთვის სათანადო წესები.

სარეზერვო ასლის შექმნა და მონაცემთა აღდგენა

პოლიტიკის მიზანი

სარეზერვო ასლის შექმნისა და მონაცემთა აღდგენის პოლიტიკის მიზანს წარმოადგენს უნივერსიტეტის კომპიუტერული და ინფორმაციული რესურსების სარეზერვო ასლების შექმნისა და მონაცემთა აღდგენის განაწესის ჩამოყალიბება.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის კომპიუტერულ და ინფორმაციულ რესურსებზე არსებულ მონაცემებზე.

ზოგადი დებულებები

უნივერსიტეტის ინფორმაციული უსაფრთხოების უზრუნველყოფისათვის მნიშვნელოვანია უნივერსიტეტის განკარგულებაში არსებული საინფორმაციო რესურსების სარეზერვო ასლების შექმნა/აღდგენა და დაზიანებულ მონაცემთა აღდგენა.

სახელმძღვანელო მითითებები

სარეზერვო ასლები იქმნება პერიოდულად და ინახება უსაფრთხო ადგილზე. შენახვის მიზანია:

- აპარატურულ-პროგრამული უზრუნველყოფის დაზიანების ან რაიმე ფორსმაჟორული სიტუაციის შემთხვევაში მონაცემთა აღდგენა;
- უზრუნველყოს მომხმარებელთა შემთხვევითი შეცდომისა ან ვირუსული და საზიანო პროგრამებით მიყენებული ზიანის გამოსწორება;
- სარეზერვო ასლების რეგულარული შექმნა საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ დაწესებული გრაფიკის მიხედვით.

სარეზერვო ასლები შეიძლება იყოს სრული და დაგროვებადი, რომელიც იქმნება პერიოდულად. სარეზერვო ასლების შექმნის სტანდარტული პროცედურებია:

- დაგროვებადი სარეზევო ასლები იქმნება ყოველდღიურად და ნარჩუნდება ერთი კვირის განმავლობაში, შემდეგ კი – ნადგურდება;
- სრული სარეზერვო ასლები იქმნება თვეში ერთხელ და ინახება 1 წლით;
- ყველა სარეზერვო მედიამოწყობილობა, რომელიც ერთჯერადი გამოყენებისაა საფუძვლიანად უნდა განადგურდეს, ხოლო მრავალჯერადი გამოყენების სარეზერვო მედიამოწყობილობა უნდა გასუფთავდეს;
- მონაცემთა მთლიანობის შენარჩუნებისა და საჭიროების შემთხვევაში აღდგენის მიზნით სრულდება სარეზერვო ასლების პერიოდული შემოწმება;
- ყოველი სერვერის სარეზერვო ასლის შენახვის გრაფიკი ინახება ელექტრონული ცხრილის დოკუმენტში.

ელექტრონულ მონაცემთა განკარგვა

პოლიტიკის მიზანი

ელექტრონულ მონაცემთა განკარგვის პოლიტიკა განსაზღვრავს უნივერსიტეტის კომპიუტერებისა და ციფრული შენახვის მოწყობილობების: გადაადგილების, შეკეთების, ჩამოწერისა თუ აღდგენის დროს ელექტრონულ მონაცემთა სათანადო მართვის განაწესს.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საკუთრებაში არსებული ყველა კომპიუტერსა და ციფრული შენახვის მოწყობილობაზე.

ზოგადი დებულებები

უნივერსიტეტი ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის დანიშნულებაა კონფიდენციალური მონაცემების დაცვა და პროგრამული უზრუნველყოფის სალიცენზიო შეთანხმებების შესრულების უზრუნველყოფა, ამიტომ მნიშვნელოვანია უნივერსიტეტის ელექტრონულ მონაცემთა განკარგვა კომპიუტერული რესურსების გადაადგილების დროს.

სახელმძღვანელო მითითებები

უნივერსიტეტის საკუთრებაში არსებული ყველა კომპიუტერი და ციფრული შენახვის მოწყობილობა უნდა იქნეს შესაბამისად დამუშავებული, სანამ მოხდება მათი საკუთრების ფორმის შეცვლა (როგორიცაა, მაგრამ არ შემოიფარგლება: გაყიდვა, გაჩუქება, ჩამოწერა და ა.შ.). კომპიუტერებისა და ციფრული საცავების მოწყობილობების დამუშავების დროს უნდა წაიშალოს მოწყობილობებზე უნივერსიტეტთან დაკავშირებული ყველა მონაცემები და ლიცენზირებული პროგრამული უზრუნველყოფა ან ფიზიკურად განადგურდეს თვით მოწყობილობა.

- ყველა კომპიუტერი და ციფრული შენახვის მოწყობილობა რომელსაც უნდა შეეცვალოს საკუთრების ფორმს დასამუშავებლად უნდა მიეწოდოს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურს;
- უნივერსიტეტის ყველა თანამშრომელი პასუხისმგებელია ერთჯერადი ციფრული შენახვის მოწყობილობების განადგურებაზე. ერთჯერადი შენახვის მოწყობილობები უნდა გაანადგურეს ფიზიკურად;
- თუ მყარი დისკი დაზიანებულია ან უმოქმედობით აღარ შეიძლება მისი გამოყენება, საჭიროა მისი დაშლა და ფიზიკური განადგურება.
- ჩამოწერისათვის მზა ყველა კომპიუტერი და შენახვის მოწყობილობა ინახება უსაფრთხო ადგილას;
- თუ მესამე მხარე იყენებს უნივერსიტეტის კომპიუტერულ მოწყობილობებს, მათ უნდა დაიცვან უნივერსიტეტის ელექტრონული მონაცემთა განკარგვის პოლიტიკა.

ინტერნეტმისამართის განაწილება

პოლიტიკის მიზანი

ინტერნეტის მისამართების განაწილების პოლიტიკის მიზანია მოახდინოს უნივერსიტეტის კომპიუტერული რესურსებისათვის ინტერნეტის მისამართების გამოყოფის განაწესის შემუშავება.

გავრცელების არე

პოლიტიკა ვრცელდება საუნივერსიტეტო კომპიუტერულ ქსელში ჩართულ მოწყობილობებზე

ზოგადი დებულებები

საუნივერსიტეტო კომპიუტერულ ქსელში მონაცემთა გადაცემა ორგანიზებულია ინტერნეტ განაწესით, ამიტომ მასში ჩართულ ყველა მოწყობილობას აქვს (უნდა მიენიჭოს) შესაბამისი (IP v4) მისამართი.

სახელმძღვანელო მითითებები

კომპიუტერული მოწყობილობების ინტერნეტის (IP) მისამართების განაწილება ხდება ცენტრალიზებულად უნივერსიტეტის ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ. სხვაგვარად მინიჭებული (IP) მისამართების მქონე მოწყობილობები დაუყოვნებლივ უნდა გაითიშოს უნივერსიტეტის ქსელიდან.

- ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური უფლებამოსილია წვდომა ქონდეს ქსელში ჩართულ ნებისმიერ მოწყობილობასთან IP მისამართის მისანიჭებლად;
- ქსელში ჩართულ მოწყობილობებს შეიძლება მიენიჭოს დინამიკური ან სტატიკური IP მისამართი: სტატიკური IP მისამართების მინიჭების საკითხი წინასწარ განიხილება ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ; დინამიკურად IP მისამართების მინიჭება ხდება საუნივერსიტეტო ქსელში ჩართული სპეციალიზირებული ქსელური მოწყობილობის ან სერვერის მეშვეობით (DHCP პროტოკოლის გამოყენებით).
- ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური აწარმოებს IP მისამართის განაწილების დოკუმენტაციას.

კომპიუტერული ქსელის მონიტორინგი

პოლიტიკის მიზანი

კომპიუტერული ქსელის მონიტორინგის პოლიტიკის მიზანია უნივერსიტეტის კომპიუტერულ ქსელში გადაცემული მონაცემების ანალიზის, აღწერისა და შესაბამისი ჩანაწერების წარმოების წესების განსაზღვრა.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საზოგადოების ყველა წევრზე და ქსელურ მოწყობილობებზე, რომლებიც ახდენენ კომპიუტერული ქსელის გამოყენებას.

ზოგადი დებულებები

უნივერსიტეტი იტოვებს უფლებას შეამოწმოს და განიხილოს მისი კომპიუტერული სისტემებისა და ქსელების ყველა მხარე, მათ შორის ინდივიდუალური სესიებისა და ანგარიშის ფაილები. ამ შემოწმების მიზანია გამოავლინოს კომპიუტერული ქსელის პრობლემები, ვირუსები და სხვა საზიანო პროგრამები, დაადგინოს, არღვევს თუ არა მომხმარებელი უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას ან სახელმწიფო კანონმდებლობას.

სახელმძღვანელო დებულებები

- უნივერსიტეტის ქსელში ჩართული ყველა კომპიუტერული და საკომუნიკაციო საშუალება ექვემდებარება ამ პოლიტიკას, იმის და მიუხედავად არის თუ არა ეს მოწყობილობა უნივერსიტეტის საკუთრება;
- უნივერსიტეტის ქსელის, ინტერნეტკავშირისა ან უნივერსიტეტის კომპიუტერული რესურსების მონიტორინგი შეუძლია განახორციელოს მხოლოდ ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურს.
- მომხმარებელმა პატივი უნდა სცეს სხვა მომხმარებელთა უფლებებს მის მონაცემებთან დაკავშირებით და არ უნდა განახორციელოს ან სცადოს ქსელის მონიტორინგი.
- უნივერსიტეტის ქსელისა და ინტერნეტის შემოწმების უფლებამოსილმა პერსონალმა არ უნდა გაამჟღავნოს ქსელის მონიტორინგის პროცესში მიღებული ინფორმაცია უნივერსიტეტის ადმინისტრაციის ნებართვის გარეშე.
- ინფორმაციული ტექნოლოგიების სამსახურის მიერ ჩატარებული კომპიუტერული ქსელის მონიტორინგის ჩანაწერები ინახება ანალიზის მიზნით.

ქსელური მარშრუტიზატორის დაცვა

პოლიტიკის მიზანი

მარშრუტიზატორის დაცვის პოლიტიკა აღწერს საჭირო მინიმალური უსაფრთხოების კონფიგურაციას უნივერსიტეტის კომპიუტერული ქსელის ყველა მარშრუტიზატორისათვის.

გავრცელების არე

ეს პოლიტიკა ვრცელდება უნივერსიტეტის კომპიუტერულ ქსელთან დაკავშირებული ყველა მარშრუტიზატორზე.

ზოგადი დებულებები

საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახური პასუხისმგებელია უნივერსიტეტის ქსელთან დაკავშირებულ ყველა მარშრუტიზატორის პარამეტრების დაყენების, მართვის, მონიტორინგისა და აუდიტის ჩატარებაზე. ასევე უფლებამოსილია გააუქმოს ყველა ის მარშრუტიზატორი, რომელიც მისი დაყენებული არაა.

სახელმძღვანელო დებულებები

ყოველი მარშრუტიზატორისათვის უნდა იყოს დაცული უსაფრთხოების შემდეგი სტანდარტები:

- წვდომის პაროლი უნდა ინახებოდეს დაშიფრული ფორმით;
- მართვისა და მონიტორინგისთვის უნდა გამოიყენებოდეს სტანდარტიზებული SNMP პროტოკოლი;
- მარშრუტიზატორის დაშორებული კონფიგურირებისთვის უნდა გამოიყენებოდეს დაშიფრული (ssh) არხი;
- მარშრუტიზატორის პროგრამული განახლება და რაიმე სხვა გეგმიური სერვისული სამუშაოები, რომელიც გამოიწვევს კომპიუტერული ქსელის მუშაობის შეფერხებას უნდა განხორციელდეს არასამუშაო საათებში.

სერვერების დაცვა

პოლიტიკის მიზანი

სერვერების დაცვის პოლიტიკის მიზანია ჩამოყალიბდეს უნივერსიტეტის მფლობელობაში ან/და ექსპლუატაციაში არსებული სერვერების კონფიგურაციის სტანდარტები.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საკუთრებაში არსებულ ან/და ექსპლუატაციაში მყოფ სერვერებზე.

ზოგადი დებულებები

უნივერსიტეტის საკუთრებაში არსებული ყველა სერვერის ფუნქციონირება ხდება საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ. სერვერის დამატება/გაუქმება უნდა ხდებოდეს უნივერსიტეტის ამავე სამსახურის ხელმძღანელის ნებართვით.

სახელმძღვანელო მითითებები

- სერვერები უნდა განთავსდეს ფიზიკურად დაცულ ტერიტორიებზე და მიწვდომადი უნდა იყოს მხოლოდ უფლებამოსილი პერსონალისთვის, რადგან ფიზიკური უსაფრთხოების ალტერნატივა არ არსებობს.
- სერვერებზე უნდა იყოს აქტიური მხოლოდ ის სერვისები, რომლებიც საჭიროა მისი დანიშნულებისათვის.
- რეგულარულად უნდა ხორციელდებოდეს სერვერის ოპერაციული სისტემის უსაფრთხოების განახლებები;
- საჭიროა ყველა სერვერის რეგულარული შემოწმება ანტივირუსული პროგრამითა და მისი მონაცემთა ბაზის რეგულარული განახლება;
- მოქმედი ანგარიშები პერიოდულად უნდა შემოწმდეს და ყველა უმოქმედო ანგარიში უნდა გაუქმდეს, ანგარიშები უნდა შეიქმნას და დაცულ იქნეს/იყოს სტანდარტიზირებული სისტემით (Kerberos, NTLM, LDAP, Active Directory და სხვა).
- განსაკუთრებული ყურადღება უნდა მიექცეს პრივილეგირებულ ანგარიშებს, რომელთაც აქვთ სისტემის რესურსების გამოყენების განუსაზღვრელი უფლებები (root; Administrator). პრივილეგირებული ანგარიშის პაროლები უნდა მიეცეს მხოლოდ მთავარ ადმინისტრატორებს.
- ყველა ანგარიშის პაროლის ფორმირება უნდა შეესაბამებოდეს „პაროლის შექმნისა და გამოყენების“ პოლიტიკას.

დამცავი ეკრანის გამოყენების პოლიტიკა

პოლიტიკის მიზანი

დამცავი ეკრანის გამოყენების პოლიტიკით განისაზღვრება უნივერსიტეტის კომპიუტერული ქსელის დამცავი ეკრანის მართვის, გამოყენებისა და კონფიგურირების განაწესი.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის საკუთრებაში არსებულ ყველა დამცავ ეკრანზე.

ზოგადი დებულებები

უნივერსიტეტის კომპიუტერულ ქსელთან დამყარებულმა ყველა კავშირმა უნდა გაიაროს ქსელის დამცავი ეკრანი. გამონაკლისი შემთხვევა უნდა განისაზღვროს და დადასტურდეს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ.

სახელმძღვანელო დებულებები

- დამცავი ეკრანები საჭიროებენ პერიოდულად შემოწმებას, რაც უნდა მოიცავდეს კონფიგურაციის პარამეტრების განსაზღვრას, სერვისის ჩართვა/გამორთვას, ნებადართულ კავშირს და შესაბამისი უსაფრთხოების ზომების მიღებას.
- უნივერსიტეტის ყველა ქსელური ეკრანი უნდა იყოს ფიზიკურად განლაგებული მონაცემთა ცენტრებში და ხელმისაწვდომი მხოლოდ იმ პირებზე, რომელთა როლები და მოვალეობებია ქსელის დამცავ ეკრანზე წვდომა. ამ საიმედო სივრცეებს ასევე უნდა გააჩნდეთ სათანადო ფიზიკური უსაფრთხოების საშუალებები.
- ყველა საეჭვო საქმიანობა, რომელიც შეიძლება იყოს არასანქცირებული მიწვდომა ან უსაფრთხოების წესების დარღვევის მცდელობა უნდა აღირიცხებოდეს ჟურნალში.
- საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახური პასუხისმგებელია კომპიუტერული ქსელთან დაკავშირებულ ყველა ეკრანის დაყენება-გაუქმების, მართვის, მონიტორინგისა და აუდიტის შესრულებაზე.

უსადენო კავშირი

პოლიტიკის მიზანი

უსადენო კავშირის პოლიტიკით განსაზღვრულია უსადენო ქსელის მაქსიმალურად ეფექტური გამოყენების, უსაფრთხოებისა და მონაცემთა მთლიანობის დაცვის წესები.

გავრცელების არე

პოლიტიკა ვრცელდება უნივერსიტეტის შიდა ქსელთან უსადენო საკომუნიკაციო საშუალებებით დაკავშირებულ ნებისმიერ მოწყობილობაზე (მაგ.: ლეპტოპები, ტაბლეტები, სმარტფონები, სათამაშო კონსოლები, უკაბელო პროექტორები და სხვა).

ზოგადი დებულებები

უნივერსიტეტის უსადენო ქსელების მართვა, მონიტორინგი და ექსპლუატაცია ხდება ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურის მიერ.

სახელმძღვანელო მითითებები

- უსადენო ქსელში დაშვება შეიძლება იყოს თავისუფალი ან შეზღუდული;
- მიუხედავად იმისა უსადენო ქსელი არის შეზღუდული თუ თავისუფალი დაშვების მასთან წვდომა უნდა ხდებოდეს WPA2/PSK ტექნოლოგიით და AES შიფრაციით შესაბამისი პაროლის გამოყენებით, რათა მაქსიმალურად იქნას დაცული აღნიშნულ ქსელში გადაცემული ინფორმაცია არასანქცირებული წვდომისგან;
- უსადენო ქსელთან დასაკავშირებელ პაროლებს ადგენს ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახური.
- თავისუფალი დაშვების უსადენო ქსელის პაროლი შეიძლება გაენდოს ნებისმიერ მსურველს, დაიწეროს საინფორმაციო დაფაზე ან განთავსდეს ნებისმიერ თვალსაჩინო ადგილზე.
- შეზღუდული წვდომის უსადენო ქსელის პაროლი გაენდობა მხოლოდ საზოგადოების იმ წევრებს რომელთაც სამსახურეობრივი საქმიანობიდან გამომდინარე ჭირდებათ აღნიშნულ ქსელთან წვდომა და ისინი ვალდებული არიან საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის თანხმობის გარეშე სხვას არ გაანდონ პაროლი.

სადენიანი და უსადენო ქსელის კარადებზე წვდომა

პოლიტიკის მიზანი

სადენიანი და უსადენო ქსელის კარადებზე წვდომის პოლიტიკის მიზანია ჩამოაყალიბოს უნივერსიტეტის სადენიანი და უსადენო ქსელის კარადების დაცვის სტანდარტები და შეამციროს მათზე არასანქცირებული წვდომის შემთხვევები.

გავრცელების არე

ეს პოლიტიკა ვრცელდება უნივერსიტეტის ტერიტორიაზე განთავსებული სადენიანი და უსადენო ქსელის კარადებზე.

ზოგადი დებულებები

უნივერსიტეტის ქსელსა და გაყვანილობის კარადაზე ხელმისაწვდომობა ნებადართულია ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამსახურისა და ამ სამსახურის მიერ უფლებამოსილ პირებისათვის.

სახელმძღვანელო მითითებები

- ქსელური მოწყობილობები უნდა მოთავსდეს ჩაკეტილ კარადაში. თუ ეს შეუძლებელია, მაშინ ქსელური აპარატურა უნდა განთავსდეს ჩაკეტილ ოთახში;
- კარადაში განთავსებულ ქსელურ აპარატურაზე ფიზიკური წვდომა შეუძლია მხოლოდ საინფორმაციო ტექნოლოგიების უზრუნველყოფის სამსახურის თანამშრომლებს ან/და ამ სამსახურის მიერ განსაზღვრულ პირებს;
- ქსელურ აპარატურას უნდა ჰქონდეს შესაბამისი გარემოსდაცვითი (ტემპერატურა, ტენიანობა და სხვ.) პირობები და უწყვეტი დენის წყარო.

კონფიდენციალურობის დაცვა

პოლიტიკის მიზანი

კონფიდენციალურობის დაცვის პოლიტიკის მიზანია უნივერსიტეტის საინფორმაციო რესურსების მონაცემთა

გავრცელების არე

უნივერსიტეტის საზოგადოების წევრები, რომლებიც იყენებენ უნივერსიტეტის კომპიუტერული ქსელისა და რესურსებს.

ზოგადი დებულებები

უნივერსიტეტის კომპიუტერული ქსელი ეკუთვნის უნივერსიტეტს და იყენებს მას აკადემიური, კვლევითი და ადმინისტრაციული საქმიანობისათვის. უნივერსიტეტის ქსელში არსებული ყველა ინფორმაცია პირადია (კერძოა). მიუხედავად იმისა, რომ უნივერსიტეტის კომპიუტერული ქსელისა და რესურსების გამოყენება მკაცრად არის წვდომის უფლებებით შეზღუდული, მაინც ინფორმაციის კონფიდენციალურობა არ არის გარანტირებული.

საკუთარი კომპიუტერული რესურსებისა და მისი მომხმარებლის ანგარიშების უსაფრთხოებისათვის უნივერსიტეტი იყენებს დაცვის სხვადასხვა ზომას. მიუხედავად ამისა უნივერსიტეტი ვერ უზრუნველყოფს მომხმარებელის მონაცემთა უსაფრთხოებისა და კონფიდენციალობის აბსოლუტურ დაცვას. ამიტომ მომხმარებელმა პრაქტიკულად თავად უნდა უზრუნველყოს „მონაცემთა უსაფრთხო გამოყენება“, მათი ანგარიშების დაცვა „პაროლის შექმნისა და გამოყენების“ პოლიტიკის თანახმად.

სახელმძღვანელო მითითებები

მომხმარებელმა უნდა იცოდეს, რომ უნივერსიტეტის ქსელი და კომპიუტერული რესურსები არ არის აბსოლუტურად კერძო საკუთრების მქონე. მიუხედავად იმისა, რომ უნივერსიტეტი არ ახორციელებს ინფორმაციის ინდივიდუალური გამოყენების მონიტორინგს, უნივერსიტეტის ქსელისა და საინფორმაციო რესურსების ნორმალური ფუნქციონირებისათვის საჭიროა მონაცემებისა და კომუნიკაციების სარეზერვო ასლების შექმნა, მონაცემების ქეშირება, აქტიურობის დღიურის წარმოება, მოხმარების ზოგადი სქემების მონიტორინგი და სხვა ასეთ მოქმედება.

უნივერსიტეტმა შეიძლება მონიტორინგი გაუწიოს უნივერსიტეტის ქსელის ან კომპიუტერული რესურსების ინდივიდუალურ მომხმარებელთა საქმიანობასა და ანგარიშებს, მათ შორის ინდივიდუალური სესიისა და კომუნიკაციის შინაარს წინასწარი გაფრთხილების გარეშე, როცა:

- მომხმარებელი ნებაყოფლობით ხდის ხელმისაწვდომს ყველასათვის იმ ინფორმაციას, რასაც ათავსებს ინტერნეტ-რესურსით, ვებ-გვერდითა ან ბლოგების მეშვეობით;
- საჭიროა უნივერსიტეტის კომპიუტერული რესურსების მთლიანობის, უსაფრთხოებისა ან ფუნქციონირების დაცვის უზრუნველყოფა;
- არსებობს იმის ეჭვი, რომ მომხმარებელმა დაარღვია ან არღვევს უნივერსიტეტის საინფორმაციო ტექნოლოგიების გამოყენების პოლიტიკას;
- ჩანს, რომ მომხმარებლის ანგარიში უჩვეულოდ აქტიურია, რაც არაა საჭირო დაშვებული უფლებებით.

კომუნიკაციის ნებისმიერი ასეთი მონიტორინგი, გარდა იმ შემთხვევებისა, რომელიც მოთხოვნილია ან მომხმარებლის მიერ, ან კანონით, ან საჭიროა გამოვლენილ საგანგებო სიტუაციაზე რეაგირება, წინასწარ უნდა იყოს დაშვებული ინფორმაციული ტექნოლოგიების სამსახურის ხელმძღვანელის მიერ. უნივერსიტეტმა, თავისი შეხედულებისამებრ შეუძლია გაამჟღავნოს ასეთი ზოგადი ან ინდივიდუალური მონიტორინგის შედეგები. მათ შორის, ინდივიდუალური კომუნიკაციების შინაარსი და ჩანაწერი უნივერსიტეტის ან სამართალდამცავი ორგანოების მოთხოვნის მიხედვით და გამოიყენოს შესაბამისი სანქციები უნივერსიტეტის შინაგანაწესის მიხედვით.