# კომპიუტერული ქსელისა და სერვერული ინფრასტრუქტურის მართვა

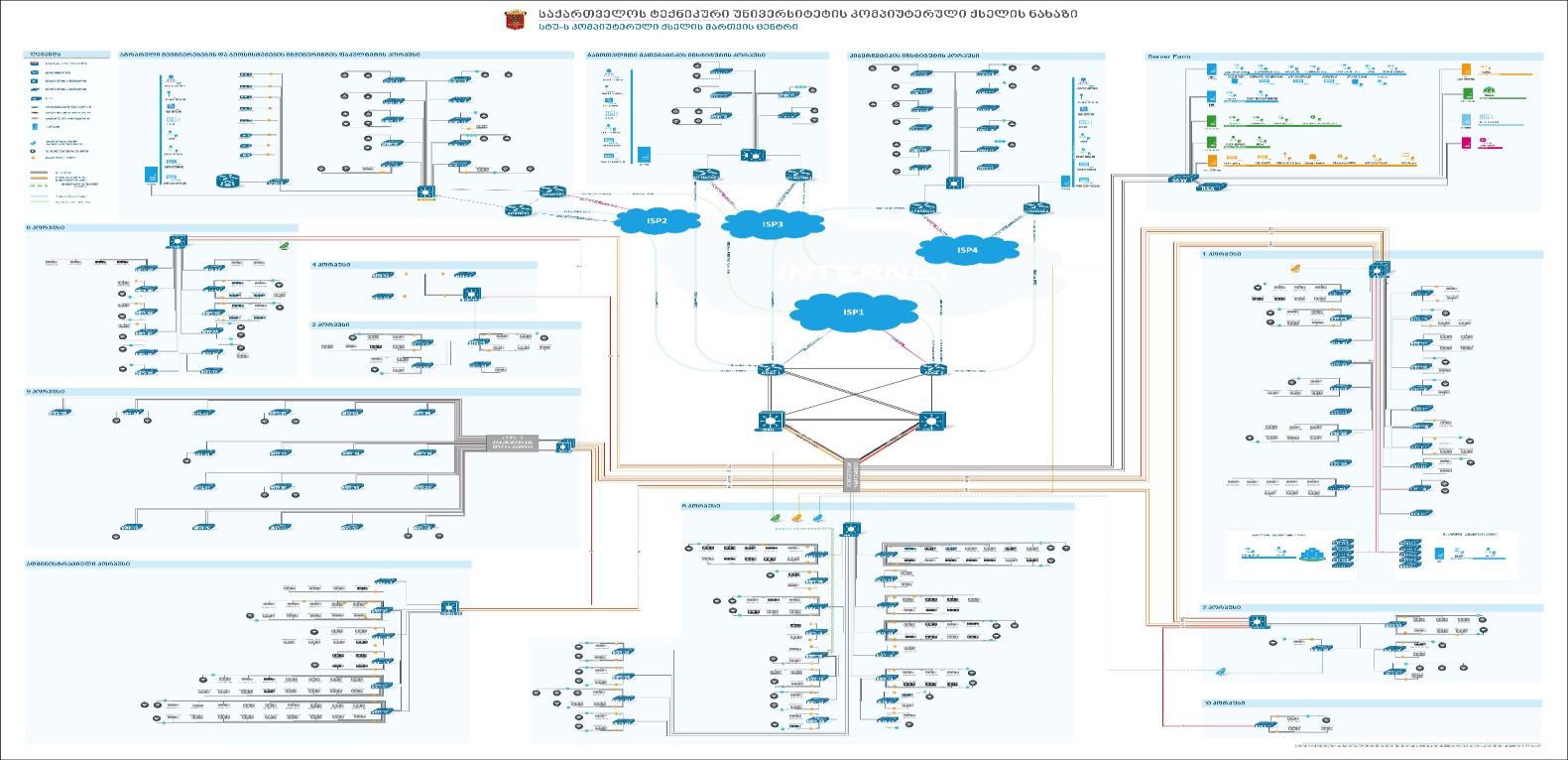
**1. კომპიუტერული ქსელის მართვა**

უნივერსიტეტის ერთიანი კომპიუტერული ქსელი არის მნიშვნელოვანი ინფორმაციული რესურსი, რომელიც გამოიყენება აკადემიური, სამეცნიერო და ადმინისტრაციული მიზნებისთვის. კომპიუტერული ქსელი აერთიანებს ინტრანეტ და ინტერნეტ სერვისებს.

# 1.1 ქსელური ინფრასტრუქტურა

1. ერთიანი კომპიუტერული ქსელი, რომელშიც ჩართულია 4000-ზე მეტი ქსელური კვანძი და ფარავს უნივერსიტეტის თითქმის მთელ სივრცეს (ყველა სასწავლო და ადმინისტრაციულ კორპუსს), სხვადასხვა ლოკაციაზე: კოსტავას ქ. № 77, გურამიშვილის გამზ. №17, სანდრო ეულის ქ.№1б, გ. ფერაძის ქ. №4 და სხვა. ასევე მისი რეგიონალური ფილიალები ტყიბულსა და დიდ ჯიხაიშში.

2. უნივერსიტეტის ყველა კორპუსი/შენობა დაკავშირებულია ოპტიკურ-ბოჭკოვანი მაგისტრალებით.



ნახ.1 სტუ-ს კომპიუტერული ქსელის სტრუქტურული სქემა.

3. უნივერსიტეტს აქვს საკუთარი BGP-ს ავტონომიური სისტემის ნომერი (AS29289) და IP მისამართები (109.205.36.0/23).

4. უნივერსიტეტში ჩართულ ყველა ქსელურ წერტილს მიეწოდება მინიმუმ 100 მბ/წმ სიჩქარის ინტერნეტი.

# 1.1.1 მართვა

უნივერსიტეტის კომპიუტერულ ქსელს მართავს უნივერსიტეტის ინფორმაციული დეპარტამენტის კომპიუტერული ქსელების მართვისა და ინფორმაციული უსაფრთხოების განყოფილება (შემდგომში - განყოფილება), რომელიც პასუხისმგებელია უნივერსიტეტის სასწავლო, ადმინისტრაციულ კორპუსებში და უნივერსიტეტის დამოუკიდებელი სამეცნიერო-კვლევითი ერთეულების შენობებში, როგორც სადენიანი, ისე უსადენო ქსელური ინფრასტრუქტურის პროექტირებაზე, საინსტალაციო სამუშაოების მონიტორინგზე და მართვაზე.

# 1.2 კომპიუტერული ქსელის მართვის პოლიტიკა

1. უნივერსიტეტის შიდა ქსელში ჩართული მოწყობილობები ექვემდებარება ერთიან უსაფრთხოების პოლიტიკას. ეს პოლიტიკა უზრუნველყოფს უნივერსიტეტის ქსელში არასანქცირებული წვდომის შეზღუდვას, რესურსების ოპტიმალურ გამოყენებას, მომხმარებელთა კომპიუტერების დაინფიცირების თავიდან აცილებას ეფექტური ანტივირუსული მექანიზმის გატარებით, არასასურველი ტრაფიკის გენერირების და სისტემაზე არასასურველი გავლენისგან დაცვას.

2. განყოფილება უზრუნველყოფს რისკების, ინფორმაციის სენსიტიურობის და უსაფრთხოების შეფასებას. განსაზღვრავს კომპიუტერის ქსელთან მიერთების და დამისამართების წესს.

# 1.2.1 უნივერსიტეტის უსადენო ქსელის ინფრასტრუქტურა და მართვის პოლიტიკა

1. უნივერსიტეტის ყველა სასწავლო კორპუსი, ადმინისტრაციული კორპუსი და დამოუკიდებელი სამეცნიერო-კვლევითი ერთეულების კორპუსები, დაფარულია უსადენო კორპორატიული ქსელური ინფრასტრუქტურით.

2. **უსადენო ქსელური ინფრასტრუქტურა (Wi-FI)**. უნივერსიტეტის მთელ პერიმეტრზე რეალიზებულია ერთიანი ცენტრალიზებული უსადენო ქსელი. უსადენო წვდომისთვის, უნივერსიტეტის კორპუსების შიდა და გარე დაფარვის ზონებისთვის, გამოყენებულია უსადენო წვდომის წერტილები. ყველა უსადენო წვდომის წერტილის მართვა და მონიტორინგი ხდება ცენტრალიზებულად, შესაბამისი კონტროლერით. უსადენო ქსელით დაფარულია საუნივერსიტეტო კორპუსების დიდი ნაწილი.

# 1.2.1.1. ფიზიკური ინფრასტრუქტურა

1. ერთიანი უსადენო კომპიუტერული ქსელი, რომელიც ფარავს უნივერსიტეტში შემავალი შენობების დერეფნებს, ბიბლიოთეკას, ეზოებს, სასწავლო და ადმინისტრაციულ ოთახს.

2. გლობალური (Public) IP მისამართები - გლობალურად ინტერნეტში მარშრუტიზებადი IP მისამართები, რომლებიც მინიჭებულია ინტერნეტ მისამართების ნუმერაციის ორგანოს (IANA) მიერ. უნივერსიტეტისთვის გამოყოფილია რეგისტრირებული 512 IP მისამართი - ქსელის მისამართი: 109.205.46.0; ქვექსელის ნიღაბი: 255.255.254.0

3. ლოკალური (Private) IP მისამართები - რომლებიც გამოიყენება შიდა დამისამართებისთვის და არ არის მარშრუტიზებადი ინტერნეტში (მოხსენიებულია [RFC1918](https://tools.ietf.org/html/rfc1918) დოკუმენტში). აღნიშნული IP მისამართებია:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

4. უნივერსიტეტის სტუდენტებისთვის (GTU STUDENTS), უსადენო ქსელში გამოყენებულია შემდეგი შეზღუდვები:

ა) სტუდენტებს უსადენო ქსელის გამოყენებით აქვთ შესაძლებლობა გამოიყენონ ყველა ის რესურსი, რომელიც საგანმანათლებლო მიზნებით არის მიზანშეწონილი, ხოლო ყველა სხვა რესურსზე წვდომა შეზღუდულია;

ბ) ინტერნეტი-ტრაფიკის სიჩქარე განისაზღვრება უნივერსიტეტის ბიზნეს და სასწავლო პროცესების სწრაფი და ხარისხიანი მომსახურეობის შესაბამისად;

გ) შეზღუდულია წვდომა უნივერსიტეტის ინტრანეტის ნაწილზე - ყველა სამართავი პანელის და კრიტიკული სერვისის სამართავ ინტერფეისზე.

5. უნივერსიტეტის სტუმრებისთვის (GTU GUEST) გამოყოფილ უსადენო ქსელში გამოყენებულია შემდეგი შეზღუდვები:

ა) შეზღუდულია წვდომა ინტერნეტთან, დახურულია ყველა სერვისი და გახსნილია წვდომა მხოლოდ იმ პორტებზე, სერვისებზე და რესურსებზე, რომლებიც საჯაროა უნივერსიტეტისთვის. ასევე გახსნილია წვდომა საგანგებო, სასწრაფო და საინფორმაციო რესურსებზე;

ბ) დახურულია ყველანაირი ტიპის გასართობი, ტორენტ და მსგავსი ტიპის საიტები;

გ) შეზღუდულია წვდომა სტუ-ს ინტრანეტზე, ყველა სამართავი პანელის და კრიტიკული სერვისის სამართავ ინტერფეისებზე;

დ) დახურულია წვდომა ყველა ადმინისტრაციულ კერძო საუნივერსიტეტო რესურსზე.

**1.3 IP მისამართების მართვის პოლიტიკა**

1. განყოფილება განკარგავს ლოკალურ დამისამართებას, გამოყოფს და ანიჭებს IP მისამართებს;

2. სისტემებს (სერვერებს), რომელთაც ჭირდებათ ინტერნეტთან პირდაპირი წვდომა და თუ აღნიშნული კავშირი კრიტიკულია სისტემისთვის - გამოეყოფა გლობალური IPv4 მისამართი;

3. განყოფილება იტოვებს უფლებას დაბლოკოს გლობალური მისამართი, თუ ამ მისამართით გაშვებული სერვისი საფრთხეს უქმნის უნივერსიტეტში ან მის გარეთ არსებულ ინფრასტრუქტურას;

4. საჭიროების შემთხვევაში, რომელიმე კონკრეტული მოწყობილობისთვის, შესაძლებელია ლოკალური IP მისამართების რეზერვირება;

5. დაუშვებელია შეთანხმების გარეშე IP მისამართების თვითნებურად გაწერა.

# 1.4 უნივერსიტეტში არსებული კომპიუტერული და ქსელური მოწყობილობების დასახელების წესი

B 06 D 306 WL 001

I სიმბოლო - სახელი იწყება ლათინური ასოთი და აღნიშნავს კორპუსს. მაგალითად: BII –III სიმბოლო აღნიშნავს კორპუსის ნომერს. მაგალითად: 06

IV სიმბოლო აღნიშნავს სექტორის იდენტიფიკატორს. მაგალითად: D

V-VII სიმბოლო აღნიშნავს ოთახის ნომერს მაგალითად: 306

VIII-IX სიმბოლო აღნიშნავს თუ ვის ეკუთვნის მოწყობილობა. მაგალითად: WL

RO - მარშრუტიზატორი; SW - კომუტატორი; SV - სერვერი;

WA - მანქანა ადმ. პერსონალის;

WL - მანქანა ლაბორატორიის;

X-XII სამ ნიშნიანი ნომერი, ოთახში მანქანის უნიკალური ნომერი, რომლის ათვლაც ხდება საათის ისრის მიმართულებით.

ზემოთ მოყვანილი მაგალითი - **B06D306WL001**

ნიშნავს ლაბორატორიის კომპიუტერს, რომელიც მდებარეობს მეექვსე სასწავლო კორპუსის 306დ ოთახში.

# საუნივერსიტეტო ქსელში მოწყობილობის ჩართვის წესი

1. კომპიუტერულ ქსელში ჩართვა ხორციელდება ადმინისტრაციის ხელმძღვანელის ან უნივერსიტეტის მიერ დანიშნული უფლებამოსილი პირის მომართვის საფუძველზე;

2. განაცხადში უნდა იყოს მოცემული კომპიუტერის განთავსების და მისი კუთვნილების შესახებ სრული ინფორმაცია;

3. კომპიუტერის ფიზიკური ადგილმდებარეობის და კუთვნილების მიხედვით იგი ერთვება უნივერსიტეტისთვის გამოყოფილ ვირტუალურ და ფიზიკურ სივრცეში;

4. სტუდენტთათვის განკუთვნილი კომპიუტერული კლასები ერთვება მათთვის ცალკე გამოყოფილ ვირტუალურ სივრცეში;

5. კომპიუტერის მიერთება ხდება მისი ადგილმდებარეობის მიხედვით, შესაბამისი უახლოესი საკომუნიკაციო კვანძის მართვად მოწყობილობასთან;

6. კომპიუტერის საუნივერსიტეტო ქსელთან მიერთების მომენტში ცნობილი უნდა იყოს მასზე განთავსებული ოპერაციული სისტემა, მისი ტექნიკური მახასიათებლები და მასზე ჩაწერილი პროგრამული უზრუნველყოფა;

7. მომხმარებელს არა აქვს უფლება თვითნებურად შეცვალოს მისთვის გამოყოფილი IP მისამართი;

8. კომპიუტერზე მისი ტექნიკური მონაცემების გათვალისწინებით უნდა იყოს გააქტიურებული ანტივირუსული პროგრამული უზრუნველყოფა;

9. ქსელური პრინტერის ინსტალაციის დროს უნდა განისაზღვროს მისი განთავსების ადგილი და რომელ ჯგუფს ემსახურება იგი;

10. უნივერსიტეტის შიდა რესურსებზე წვდომა გარე ქსელიდან ხორციელდება განყოფილების გადაწყვეტილების საფუძველზე;

11. ცენტრალური და პერიფერიული კვანძები თავსდება სატელეკომუნიკაციო ოთახებში შესაბამისი ტემპერატურული რეჟიმით ან საკომუნიკაციო კარადებში ფიზიკური უსაფრთხოების უზრუნველყოფის მიზნით;

12. ცენტრალურ და პერიფერიულ საკომუნიკაციო კვანძებთან წვდომა პრობლემების აღმოფხვრის ან გაფართოებითი სამუშაოების წარმოების დროს, ხორციელდება მხოლოდ განყოფილების ინჟინერის ან ადმინისტრატორის მიერ;

13. დაუშვებელია საუნივერსიტეტო ქსელთან თვითნებური მიერთება;

14. აკრძალულია მომხმარებლის მხრიდან, საუნივერსიტეტო ქსელში რაიმე ქსელური მოწყობილობის ჩართვა შეთანხმების გარეშე;

15. საუნივერსიტეტო ქსელში პრობლემის წარმოქმნის დროს ხორციელდება მისი ლოკალიზაცია, მიზეზის დადგენა და პრობლემის აღმოფხვრა;

16. საკომუნიკაციო კვანძებთან კომუნიკაცია უნდა ხორციელდებოდეს დაშიფრული პროტოკოლის მეშვეობით.

# 1.6 დაშვებული პორტები და სერვისები

უსაფრთხოების პოლიტიკის შესაბამისად გახსნილია მხოლოდ ის პორტები და სერვისები, რომელიც საგანმანათლებლო მიზნებისთვის არის მიზანშეწონილი და საუნივერსიტეტო ქსელის გამართული და უსაფრთხო მუშაობისთვის არის აუცილებელი.

# 1.6.1 ნებადართული პორტების ჩამონათვალი:

**TCP:** 20, 21, 25, 53, 80, 110, 143, 443, 465, 578, 993, 995, 8000-8002, 8080, 81, 8081, 7501, 4444, 9933,

2082, 2222, 13000, 1110, 2110, 2082, 2083, 989, 4244, 5222, 5223, 5228, 5242, 49152-65535

**UDP:** 53,123,5060-5070,1000-2000,9785,5243,9090,3478-3481,49152-65535

უსაფრთხოების მიზნით დახურულია გარედან წვდომა უნივერსიტეტის ქლაუდზე არსებული კრიტიკული სერვისების სამართავ ინტერფეისებზე (მათ შორის იმ სერვისებზეც, რომლის მართვას და მენეჯმენტს ახორციელებს სხვა სამსახური), ნებადართულია გარედან წვდომა მხოლოდ VPN კავშირის საშუალებით.

აღნიშნული პოლიტიკა გათვალისწინებულია იმისთვის, რომ უნივერსიტეტის კომპიუტერული ქსელი იყოს მაქსიმალურად საუნივერსიტეტო გარემოზე მორგებული, ასევე ქსელისთვის დამახასიათებელი უსაფრთხოების მაღალი რისკების გათვალისწინების და უნივერსიტეტის ინტერნეტ ტრაფიკის არა საუნივერსიტეტო მიზნებისთვის გამოყენების შესამცირებლად.

# 1.7. უსაფრთხოების, ინციდენტების აღმოჩენის და რეაგირების ტექნოლოგიები და მონიტორინგი

1. უნივერსიტეტის კომპიუტერულ ქსელში გამოყენებულია სხვადასხვა მონიტორინგის სისტემები (PRTG, DUDE, KIWI SYSLOG Server) და პროტოკოლები (snmp, Netflow, syslog). რომელთა მართვაც ხდება ცენტრალიზებულად, ქსელის ოპერაციების ცენტრში (NOC).

2. ხორციელდება ინტერნეტის ლოკალური და გლობალური ტრაფიკის, აქტიური მომხმარებლების, მოთხოვნადი სერვისებისა და პროტოკოლების მუდმივი 24/7 მონიტორინგი, რის საფუძველზეც ხდება მონაცემების შეგროვება, მათი ბაზისის გამოთვლა და უჩვეულო ტრაფიკის იდენტიფიცირება და ანალიზი. მონიტორინგის საშუალებით ხდება სხვადასხვა კიბერ-შეტევების აღმოჩენა და პრევენცია.

3. ცენტრალიზებულად ხდება ქსელის მოწყობილობების მდგრადობის და სტაბილურად მუშაობის მუდმივი მონიტორინგი სხვადასხვა სენსორების გამოყენებით (CPU-დატვირთვა, თავისუფალი RAM, ტემპერატურა და ა.შ.). ცენტრალიზებულად ხდება ყველა ლოგის (LOG) შენახვა გარკვეული დროით და პრობლემის შემთხვევაში მათი ანალიზი.

4. მონიტორინგის სისტემის მეშვეობით რეგულარულად უნდა ხორციელდებოდეს საკომუნიკაციო კვანძებზე დაკვირვება;

5. სისტემის სრული მტყუნების შემთხვევაში აღდგენის გეგმის მიხედვით ხდება ჯერ ცენტრალური კომუტაციის კვანძების აღდგენა და შემდგომ პერიფერიული მოწყობილობებთან კომუნიკაციის აღდგენა;

6. ნებისმიერი უარყოფითი მოვლენის შესახებ ინფორმაცია უნდა გადაიგზავნოს log სერვერზე.

# 2. სერვერული ინფრასტრუქტურა და მისი მართვა

1. უნივერსიტეტის სერვერული ინფრასტრუქტურა ემსახურება უნივერსიტეტში არსებული სერვისების და სამეცნიერო-კველევითი ამოცანების მხარდაჭერას.

2. უნივერსიტეტის სერვერული ინფრასტრუქტურა განთავსებულია უნივერსიტეტის სხვადასხვა ლოკაციაზე:

უნივერსიტეტის მე-9 კორპუსი, 317 ოთახი , მე-6 კორპუსი, ოთახი 306 დ, სტუ-ს პირველი კორპუსი (კომპიუტერული ცენტრი პირველი სართული), ვ. ჭავჭანიძის სახელობის კიბერნეტიკის ინსტიტუტი, ნიკო მუსხელიშვილის სახელობის გამოთვლითი მათემატიკის ინსტიტუტი და აგრარული მეცნიერებებისა და ბიოსისტემების ინჟინერინგის ფაკულტეტი.

# 2.1. ფიზიკური ინფრასტრუქტურა

1. სერვერული ინფრასტრუქტურა განთავსებულია სპეციალურ სარეკრიაციო ოთახებში, რომლებიც უზრუნველყოფილია გაგრილებით და უწყვეტი კვების მოწყობილობებით. სერვერულ ინფრასტრუქტურაში შედის სხვადასხვა ტიპის და სიმძლავრის სერვერები, რომლებიც ასრულებენ როგორც მთავარ, ასევე სხვა სერვერების სარეზერვო ფუნქციასაც.

2. ინფრასტრუქტურაში შედის სახვადასხვა ტიპის სერვერები: სტორიჯ, ბლეიდ და სტანდარტული ტიპის სერვერები.

3. სერვერულ ინფრასტრუქტურაში გამოყენებული ტექნოლოგია საშუალებას იძლევა მოხდეს სერვერების კლონირება (სარეზერვო ასლების) სხვადასხვა ფიზიკურ სერვერზე. სერვერის ფიზიკური, პროგრამული მტყუნების ან ჰაკერული თავდასხმის შემთხვევაში ინფრასტრუქტურა საშუალებას იძლევა გაეშვას სარეზერვო სერვერი.

4. სერვერული ინფრასტრუქტურა დაცულია მუდმივი კვების ელემენტებით (UPS) და გაზ-გენერატორით, რაც სისტემას საშუალებას აძლევს შენარჩუნდეს სერვერების ფუნქციონირება.

# 2.1.1. სასერვერო ინფრასტრუქტურაში გამოყენებული ტექნოლოგიები

1. სასერვერო ინფრასტრუქტურაში შემავალი სერვერების დიდი ნაწილი იმართება სერვერებისთვის განკუთვნილი ვირტუალური მანქანების სამართავი პროგრამული სისტემების გამოყენებით, ესენია VMware vSphere Hypervisor და Citrix XenServer. ინფრასტრუქტურის ფიზიკური სერვერებისთვის ზოგ შემთხვევაში გამოყენებულია UNIX, Linux და Microsoft Windows Server ოპერაციული სისტემები.

2. ინფრასტრუქტურა დაცულია ფაირვოლით.

# 2.1.2. ინფრასტრუქტურის ადმინისტრირების წესი (მართვა)

უნივერსიტეტის სერვერული და ქსელური ინფრასტრუქტურა იმართება განყოფილების მიერ. იგი პასუხისმგებელია სერვერული და ქსელური ინფრასტრუქტურის სისტემურ გამართვაზე და მის ტექნიკურ უზრუნველყოფაზე.

# 2.1.3. ფიზიკურ ინფრასტრუქტურაზე დაშვების წესი

ამ დოკუმენტში აღწერილი პროცედურები შემუშავებულია მონაცემთა ცენტრის უსაფრთხო გარემოს შესანარჩუნებლად.

მნიშვნელოვანია, რომ ნებისმიერმა განყოფილებამ/პროექტმა, რომელიც განიხილავს მონაცემთა ცენტრში თავისი სერვერების დაყენებას, სრულად გაიგოს და დაეთანხმოს ამ პროცედურებს.

1. მიმოხილვა

მონაცემთა ცენტრის უსაფრთხოება ინფორმაციული ტექნოლოგიების დეპარტამენტის პასუხისმგებლობაა. უსაფრთხოებისა და სისტემის ადმინისტრატორი პასუხისმგებელია ამ პოლიტიკის ადმინისტრირებაზე. ქვემოთ მოცემულია ზოგადი მოთხოვნები, პოლიტიკა და პრაქტიკა, რომელიც არეგულირებს წვდომას ამ მგრძნობიარე ზონაში, რაზეც პასუხისმგებელია ინფორმაციული ტექნოლოგიების დეპარტამენტი. მნიშვნელოვანია, რომ უნივერსიტეტის ყველა აკადემიურმა პესონალმა , თანამშრომლებმა და ბიზნეს პარტნიორებმა დაიცვას ეს პოლიტიკა. ამ პოლიტიკის შეუსრულებლობა ითვლება პერსონალის პასუხისმგებლობის დაკისრების საფუძვლად.

1. პირველადი სახელმძღვანელო მითითებები

„მონაცემთა ცენტრი“ არის შეზღუდული ზონა, რომელიც მოითხოვს ბევრად უფრო დიდ კონტროლს, ვიდრე ჩვეულებრივი არასაჯარო სივრცეები. ამ ტერიტორიაზე შესვლა შეუძლიათ მხოლოდ იმ პირებს, რომლებსაც აქვთ ამის უფლება. წვდომის პრივილეგიები მიენიჭება იმ პირებს, რომლებსაც აქვთ ლეგიტიმური საქმიანობის უფლება „მონაცემთა ცენტრი“ ყოფნის დროს. გარდა ამისა, ამ ტერიტორიზე ყოფნა დაშვებულია მხოლოდ უნივერსიტეტის ავტორიზებული საქმიანობის განსახორციელებლად.

მონაცემთა ცენტრის უსაფრთხოების პოლიტიკასა და პრაქტიკაში დაშვებული ერთადერთი გამონაკლისი არის ამ წესების დროებითი შეჩერება, თუ საჭირო გახდება სამედიცინო, სახანძრო და/ან პოლიციის თანამდებობის პირებისთვის და ა.შ.

1. მონაცემთა ცენტრზე წვდომის დონეები

მონაცემთა ცენტრში არის 3 „წვდომის დონე“:

* **ზოგადი წვდომა**
* **შეზღუდული წვდომა**
* **თანხლებით წვდომა**

ზოგადი წვდომა

ზოგადი წვდომა ეძლევა ადამიანებს, რომლებსაც აქვთ მონაცემთა ცენტრში წვდომის უფლება. ზოგადი ხელმისაწვდომობა ენიჭება ინფორმაციული ტექნოლოგიების პერსონალს, რომელთა სამუშაო პასუხისმგებლობები მოითხოვს მათ წვდომას ამ ტერიტორიაზე.

პირებს, რომლებსაც აქვთ ზოგადი წვდომა, შეუძლიათ წვდომა საინფორმაციო ტექნოლოგიების მონაცემთა ცენტრსა და კატასტროფის აღდგენის ზონებში გასაღების წვდომის საშუალებით.

იმ პირებს, რომლებსაც აქვთ საერთო წვდომა ტერიტორიასთან, შეიძლება დაუშვან სათანადო უფლებამოსილი პირების თანხლებით წვდომა მონაცემთა ცენტრში.

თანხლებით წვდომა

თანხლებით წვდომა არის მჭიდროდ მონიტორინგის ქვეშ მყოფი წვდომა, რომელიც ეძლევა ადამიანებს, რომლებსაც აქვთ ლეგიტიმური ბიზნეს მოთხოვნილება მონაცემთა ცენტრში იშვიათი წვდომისთვის. "იშვიათი წვდომა" ზოგადად განისაზღვრება, როგორც წვდომა, რომელიც საჭიროა წელიწადში 15 დღეზე ნაკლებ დროზე.

პირი, რომელსაც აქვს თანხლებით წვდომა ტერიტორიაზე, უნდა შევიდეს და გამოვიდეს ზოგადი წვდომის მქონე პირის უშუალო მეთვალყურეობის ქვეშ.

შეზღუდული წვდომა

შეზღუდული წვდომა ენიჭება პირს, რომელსაც არ აქვს ზოგადი წვდომის კვალიფიკაცია, მაგრამ აქვს ლეგიტიმური საქმიანი მიზეზი მონაცემთა ცენტრზე ზედამხედველობის გარეშე წვდომისთვის. მას არ შეუძლია უფლება მისცეს სხვებს, მიენიჭონ მონაცემთა ცენტრში უკონტროლო წვდომა.

1. მონაცემთა ცენტრის კარი

მონაცემთა ცენტრის ყველა კარი მუდამ უნდა იყოს ჩაკეტილი და შეიძლება მხოლოდ დროებით გაიხსნას იმ პერიოდის განმავლობაში, რომელიც არ აღემატება მინიმალურად აუცილებელ დროს.

მონაცემთა ცენტრში კარი იღება მხოლოდ იმ შემთხვევაში, თუ საჭიროა ჰაერის ნაკადის გაზრდა მონაცემთა ცენტრში კონდიცირების გაუმართაობის შემთხვევაში. ამ შემთხვევაში, ინფორმაციული ტექნოლოგიების დეპარტამენტის წვდომის მქონე პერსონალი უნდა იყოს და შეზღუდოს მონაცემთა ცენტრში წვდომა.

1. გამონაკლისის ანგარიშგება

მონაცემთა ცენტრის ფიზიკური უსაფრთხოების პოლიტიკისა და პროცედურების ყველა დარღვევა საჭიროების შემთხვევაში უნდა ეცნობოს (მაგ.: საგანგებო, გარდაუვალი საფრთხე და ა.შ.) კორპუსის დაცვას რაც შეიძლება მალე.

როდესაც მონაცემთა ცენტრში აღმოჩენილია არაავტორიზებული პირი, ის დაუყოვნებლივ უნდა ეცნობოს ინფორმაციული ტექნოლოგიების გუნდის წევრს. თუ ეს მოხდება საღამოს საათებში, უნდა დაუკავშირდეთ უფროს მენეჯმენტს. ისინი დაადგენენ, უნდა დაუკავშირდნენ თუ არა კორპუსის დაცვას.

არაუფლებამოსილი პირი დაცვის სამსახურის თანამშრომლის მიერ უნდა იყოს გამოყვანილი ტერიტორიიდან.

# 2.2. სერვერული ინფრასტრუქტურის მონაცემთა უსაფრთხოება

1. უნივერსიტეტის სერვერებზე განთავსებული ინფორმაციის ასლები ინახება სარეზერვო ფიზიკური სერვერის მონაცემთა საცავებში .

2. კრიტიკულ სერვისებზე უნდა განხორციელდეს სარეზერვო ასლების შექმნა:

ა) კრიტიკულად მნიშვნელოვანი სერვისების (რომელზეც დღეში რამდენიმეჯერ შედის ცვლილება) დღეში ერთხელ, ზოგ შემთხვევაში დღეში 5-ჯერ მოხდეს მონაცემთა ბაზების და სხვა მონაცემების არქივირება;

ბ) სხვა შემთხვევაში მონაცემთა არქივირება უნდა განხორციელდეს კვირაში ერთხელ.

# 2.2.1. ინფრასტრუქტურაში პაროლების შენახვის და გამოყენების წესი

ყველა პაროლი ინახება ამ მიზნისთვის გამოყოფილ სპეციალურ დაცულ ადგილას და ის ხელმისაწვდომია მხოლოდ უფლებამოსილი თანამშრომლებისთვის.