სსიპ - ივანე ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტის
ადმინისტრაციის ხელმძღვანელის
2018 წლის 23 თებერვლის N35/02-01 ბრძანების დანართი N1
დანართი 1

სსიპ - ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ინფორმაციული ტექნოლოგიების მართვის პოლიტიკა და საინფორმაციო რესურსების გამოყენების წესი

პრეამბულა

საინფორმაციო ტექნოლოგიების რესურსები სხვადასხვა ელექტრონულ საშუალებებს, რომლებიც მომხმარებელს საკუთარი საქმიანობის ეფექტურობის გაზრდის და გარკვეული დამატებითი ფუნქციების შესრულების საშუალებას აძლევს.
კორპორატიული რესურსებით სარგებლობის მოთხოვნის უფლება აქვს უნივერსიტეტის ყველა თანამშრომელს მისი სამუშაო პოზიციის მიხედვით.
თანამშრომლის პოზიციის სპეციფიკიდან გამომდინარე მომხმარებელს შეუძლია მოითხოვოს სხვადასხვა რესურსებით სარგებლობის უფლება არსებული, ახალი ან დროებითი მომხმარებლებისათვის.
შეიძლება განაცხადის გაკეთება უნივერსიტეტის შემდეგი რესურსებისთვის:
ა) ელექტრონული ფოსტა;
ბ) ფაილური რესურსი (ე.წ. Z:-დისკი);
გ) დისტანციური წვდომა უნივერსიტეტის შიდა საინფორმაციო სერვისებზე (VPN);
დ) ინტერნეტი;
ე) ვებ-ჰოსტინგი და სხვა.
საქმიანობის საჭიროებებიდან გამომდინარე, უნივერსიტეტის თანამშრომლებს საშუალება აქვთ მოითხოვონ დამატებითი უფლებები უნივერსიტეტის საინფორმაციო რესურსებზე, რისთვისაც აუცილებელია:
ა) განაცხადის შევსება დამატებითი საუნივერსიტეტო ინფორმაციული რესურსებით სარგებლობის შესახებ;
ბ) განაცხადის ფორმაზე უშუალო ხელმძღვანელის ხელმოწერა;
განაცხადის მიწოდება უნივერსიტეტის საინფორმაციო ტექნოლოგიების მართვის დეპარტამენტისთვის.
გ) კორპორატიული რესურსებით სარგებლობის მოთხოვნა განიხილება საინფორმაციო ტექნოლოგიების დეპარტამენტში და დადგენილ ვადებში მომთხოვნს მიეწოდება ინფორმაცია მოთხოვნის დაკმაყოფილება/არდაკმაყოფილების შესახებ.
მუხლი 1. ინტერნეტის გამოყენება, ზოგადი წესები
1. ინტერნეტი ნებისმიერ ორგანიზაციაში მაღალი მნიშვნელობის მქონე სამუშაო და საკომუნიკაციო საშუალებას წარმოადგენს. მისი გამოყენება აუცილებელია ორგანიზაციის სამუშაო პროცესის ეფექტიანად წარმართვისთვის.
2. წინამდებარე წესი აღწერს უნივერსიტეტში ინტერნეტის გამოყენების წესებს და მათი დაცვის მეთოდებს. წესის მოქმედება ვრცელდება ყველა მოხმარებელზე, რომელიც უნივერსიტეტის IT-ინფრასტრუქტურის ფარგლებიდან ინტერნეტთან წვდომას

ახორციელებს. უნივერსიტეტში ინტერნეტის მომხმარებელთა შემდეგი ტიპები არსებობს:

ა) ადმინისტრაციული და აკადემიური პერსონალი;
ბ) სტუდენტები;
გ) უნივერსიტეტის სტუმრები.
3. უნივერსიტეტს IT-ინფრასტრუქტურაში იგულისხმება როგორც უშუალოდ უნივერსიტეტში ფიზიკურად განთავსებული, ასევე გარე გამოთვლითი რესურსები (პერსონალური კომპიუტერები, მობილური მოწყობილობები), რომლებიც ინტერნეტთან წვდომას უნივერსიტეტის არხების გავლით ახორციელებენ.
4. ინტერნეტით მომსახურების ძირითად მიზანს მომხმარებელთა სამუშაო პროცესისთვის აუცილებელი გარე ინფორმაციით და სერვისებით უზრუნველყოფა წარმოადგენს. ინტერნეტ-სერვისის არადანიშნულებისამებრ გამოყენებამ შეიძლება სხვადასხვა ტიპის უსაფრთოების რისკ-ფაქტორები წარმოშვას, რომლებიც აფერხებენ როგორც უნივერსიტეტის ინტერნეტით მომსახურებას, ასევე, რიგ შემთხვევებში, მთელი IT-ინფრასტრუქტურის გამართულ მუშაობას. ზოგიერთ რისკ-ფაქტორს შეუძლია უნივერსიტეტის მიმართ სამართლებრივი პრობლემების წარმოქმნა გამოიწვიოს.
5. ინტერნეტით სარგებლობის წესის შემოღების ძირითად მიზნებს წარმოადგენს:
ა) უნივერსიტეტის ონლაინ-უსაფრთხოების რისკების შემცირება;
ბ) მომხმარებელთა ინფორმირება ინტერნეტში დაშვებული და აკრძალული მოქმედებების შესახებ;
გ) მომხმარებელთა ინფორმირება წესების დარღვევის შემთხვევაში შესაძლო სანქციების შესახებ;
დ) უნივერსიტეტის ინტერნეტ-სერვისის გამოყენება მხოლოდ ავტორიზებული მომხმარებლებისთვის დაიშვება;
ე) მომხმარებელი ავტორიზებული ხდება უნივერსიტეტში საქმიანობის დაწყებისთანავე და კარგავს ავტორიზაციას უნივერსიტეტში საქმიანობის დასრულებისთანავე.
6. უნივერსიტეტს ინტერნეტ-სერვისის მომხმარებლები ვალდებულნი არიან:
ა) გამოიყენონ ინტერნეტი სამსახურეობრივი მიზნებისთვის;
ბ) ყურადღებით მოეპყრონ უნივერსიტეტის ქსელიდან (და უნივერსიტეტის სახელით) მათ მიერ ინტერნეტში გაგზავნილ ინფორმაციას, უზრუნველყონ მისი ეთიკურობა და ლეგალურობა;
გ) იმუშაონ მხოლოდ მათთვის შექმნილი აუთენტიფიკაციის მონაცემებით, არ გამოიყენონ სხვა მომხმარებლებლების აუთენტიფიკაციის მონაცემები;
7. ინტერნეტ-სერვისის მოხმარებლებს ეკრძალებათ:
ა) უნივერსიტეტის ინტერნეტ-სერვისის გამოყენება ისეთი ონლაინ-საქმიანობისთვის, რაც საფრთხეს უქმნის მთლიანად ორგანიზაციის რეპუტაციას (მ.შ. ინტერნეტის გამოყენება არალეგალური ან/და კრიმინალური საქმიანობისთვის);
ბ) ისეთი კონტენტის შექმნა და უნივერსიტეტის ინტერნეტ-არხებით გავრცელება, რომელსაც ორგანიზაციისთვის სამართლებრივი პრობლემების მოტანა შეუძლია;
გ) დაუშვებელი ინფორმაციული კონტენტის ჩამოტვირთვა, შექმნა, ნახვა და გავრცელება (პორნოგრაფია, რასისტული, შეურაცხმყოფელი ან რეპუტაციის შემლახველი, კრიმინალთან და ექსტრემიზმთან ასოცირებული კონტენტი);

დ) საავტორო უფლებებით დაცული კონტენტის (ფილმები, მუსიკა, წიგნები, პროგრამული უზრუნველყოფა და სხვა) ჩამოტვირთვა, ნახვა და გავრცელება.
ე) მავნე პროგრამული უზრუნველყოფის შეგნებულად ჩამოტვირთვა და გავრცელება საუნივერსიტეტო IT-სივრცეში;
ვ) სათამაშო (მათ შორის აზარტული თამაშების) გვერდებზე შესვლა და მუშაობა;
ზ) უნივერსიტეტისთვის კრიტიკული ინფორმაციული კონტენტის ტრანსპორტირება ინტერნეტში დაუცველი (შეუმოწმებელი) არხებით;
თ) უნივერსიტეტის ინტერნეტთან კავშირის არხების გადატვირთვა ქსელურ რესურსებზე მაღალი მოთხოვნის მქონე პროგრამებით და სერვისებით (ვიდეოპორტალები, კონტენტის ჩამოტვირთვის სერვისები, სოციალური ქსელები, ტორენტ-კლინტები და სხვა).
ი) წესებში გამონაკლისების დაშვება შესაძლებელია მხოლოდ უნივერსიტეტის ადმინისტრაციის ნებართვით, განცხადების საფუძველზე.
8. ინტერნეტის გამოყენება დასაშვებ ფარგლებში ინტერნეტის პირადი მიზნებისთვის გამოყენება ნებადართულია შემდეგი წესების დაცვით:
ა) ინტერნეტის პირადი მიზნებით გამოყენების პერიოდი არ უნდა ემთხვეოდეს სამუშაო საათებს (დასაშვებ პერიოდებია შუადღის შესვენება და არასამუშაო საათები);
ბ) ინტერნეტის პირადი მიზნით გამოყენება არ უნდა არღვევდეს ინტერნეტის გამოყენების საერთო წესებს.
მუხლი 2. ინტერნეტით სარგებლობის წესის დანერგვა
1. ინტერნეტით სარგებლობის წესის დანერგვას და მონიტორინგს უზრუნველყოფს უნივერსიტეტის საინფორმაციო ტექნოლოგიების დეპარტამენტი.
2. დანერგვის ინსტრუმენტს წარმოადგენს სპეციალიზებული აპარატურა და პროგრამული უზრუნველყოფა (ფაიერვოლი, პროქსი-სერვერი, ანტივირუსი), რომელთა საშუალებით სრულდება სხვადასხვა ტიპის ქსელური პროტოკოლების, აპლიკაციებისა და მომხმარებლებისთვის ინტერნეტთან წვდომის უფლებების განსაზღვრა და მართვა, აგრეთვე ჩამოტვირთული ინფორმაციის შემოწმება ვირუსებსა და სხვა მავნე პროგრამების არსებობაზე.
მუხლი 3. მონიტორინგი და შესაძლო სანქციები
1. უნივერსიტეტის საინფორმაციო ტექნოლოგიების დეპარტამენტი უფლებამოსილია აწარმოოს მომხმარებელთა მიერ ინტერნეტის გამოყენების მონიტორინგი და აუცილებლობის შემთხვევაში გაატაროს სანქციები.
2. ინტერნეტის წესის დარღვევის შემთხვევაში უნივერსიტეტის საინფორმაციო ტექნოლოგიების დეპარტამენტი უფლებამოსილია ინტერნეტის მომხმარებლებს ან მომხმარებელთა ჯგუფების მიმართ შემდეგი ტიპის სანქციები გაატაროს:
ა) ინტერნეტის ტრაფიკის მოხმარების შეზღუდვა;
ბ) ინტერნეტით სარგებლობის უფლების ჩამორთმევა;
გ) საჭიროების შემთხვევაში უნივერსიტეტის ადმინისტრაციის ინფორმირება შემდგომი რეაგირებისთვის.

მუხლი 4. ელექტრონული ფოსტის გამოყენების წესი
1. ელექტრონული ფოსტის მისამართით უზრუნველყოფილ უნდა იქნას უნივერსიტეტის ყველა თანამშრომელი, ხელშეკრულების გაფორმებისთანავე, წერილობითი მომართვის საფუძველზე.

2. უნივერსიტეტის კორპორატიული ელექტრონული ფოსტის მისამართის მინიჭება შეიძლება მოხდეს გარკვეულ მომხმარებელთათვისაც, წერილობითი მომართვის საფუძველზე.
3. მომხმარებელთა ჯგუფებისთვის ელექტრონული ფოსტის მისამართი შეიძლება იყოს სამი ტიპის: შეზღუდული ჯგუფური, ჯგუფური და ინდივიდუალური. ორივე ტიპი კორპორატიულ ელექტრონული ფოსტის სახეობას განეკუთვნება, მაგრამ მათი გამოყენების არეალი განსხვავებულია.
4. შეზღუდული ჯგუფური ელექტრონული ფოსტის მისამართები განკუთვნილია ორგანიზაციის ფარგლებში საერთო, მნიშვნელოვანი ინფორმაციის დასაგზავნად. აღნიშნული ტიპის მისამართებს ტექნიკურად მართავს საინფორმაციო ტექნოლოგიების დეპარტამენტი, შინაარსობრივად - საზოგადოებასთან ურთიერთობის დეპარტამენტი.
5. ჯგუფური ელექტრონული ფოსტის მისამართი გამოიყენება შიდა კომუნიკაციისათვის უნივერსიტეტის თანამშრომლებს შორის. ასეთი ელექტრონული მისამართით შესაძლებელია წერილების ჯგუფურად დაგზავნა, ხოლო მათი მიღება შეზღუდულია არაავტორიზებული მომხმარებლებისთვის.
6. ინდივიდუალური ელექტრონული ფოსტის მისამართი – გამოიყენება დანიშნულებიდან გამომდინარე კორესპონდენციის საწარმოებლად, როგორც ქსელის გარეთ, ასევე შიგნით.
7. თანამშრომელთა ინდივიდუალური ელექტრონული ფოსტის მისამართი შემდეგ სახეს ატარებს:
ა) <სახელი.გვარი>@tsu.ge. სტუდენტების (ბაკალავრიატის სტუდენტები, მაგისტრანტები, დოქტორანდები)
8. ელექტრონული ფოსტის მისამართი ატარებს შემდეგ სახეს:
ა) <სახელი.გვარი.პირადი ნომრის ბოლო სამი ციფრი>@tsu.ge
9. უნივერსიტეტის ელექტრონული ფოსტის სისტემა განკუთვნილია მხოლოდ საქმიანი კომუნიკაციისათვის და არავითარ შემთხვევში პირადი სარგებლობისათვის. უნივერსიტეტი იტოვებს უფლებას მონიტორინგი გაუწიოს ელექტრონული ფოსტით სარგებლობას, რათა დარწმუნდეს, რომ თანამშრომელი ბოროტად არ იყენებს კორპორატიულ ელექტრონულ ფოსტას.
10. თუ რომელიმე თანამშრომელს/სტრუქტურულ ერთეულს სჭირდება გარკვეული ინფორმაციის დაგზავნა შეზღუდული ჯგუფურ ელექტრონული ფოსტის მისამართებზე და ეს ერთჯერად მოქმედებას წარმოადგენს, მან აღნიშნული ინფორმაციის დაგზავნის შესახებ მენეჯმენტისაგან მიღებული თანხმობა და ინფორმაცია უნდა გადაუგზავნოს საზოგადოებასთან ურთიერთობის დეპარტამენტს მისი შემდგომი დაგზავნის მიზნით.
11. დეპარტამენტების/სტრუქტურული ერთეულის უფროსებს უფლება აქვთ წერილი გააგზავნონ სტრუქტურულად მათ დაქვემდებარებაში მყოფ პოზიციური ნიშნით გაერთიანებულ შეზღუდულ ელექტრონული ფოსტის ჯგუფებზე.
12. თუ რიგით თანამშრომელს აღნიშნულ შეზღუდულ ელექტრონული ფოსტის მისამართებზე ინფორმაციის დაგზავნის აუცილებლობა (საქმიანობის სფეროდან გამომდინარე) წარმოექმნება სისტემატიურად, შესაბამისი უფლების მისაღებად წერილობით უნდა მიმართოს უნივერსიტეტის საინფორმაციო ტექნოლოგიების დეპარტამენტს.

13. ელექტრონული მისამართი წარმოადგენს უნივერსიტეტის თანამშრომლის ოფიციალურ საკონტაქტო ინფორმაციას და ყველა საქმიანი კორესპონდენცია უნდა გაგზავნილი იქნეს მხოლოდ ამ მისამართზე.

14. თანამშრომლის სამსახურიდან წასვლის შემდეგ მისი ელექტრონული ფოსტის მისამართი რჩება აქტიური 6 თვის განმავლობაში, რის შემდეგაც მისი ანგარიში იბლოკება და ინახება არქივის სახით. გამონაკლის შემთხვევაში, წერილობითი მომართვის საფუძველზე, შესაძლებელია სამსახურიდან წასული თანაშრომლის მეილის აქტიურ მდგომარეობაში დატოვება მეტი ხნით.
15. უნივერსიტეტის უსაფრთხოების უზრუნველყოფის პრაქტიკიდან გამომდინარე, ხდება ელექტრონული საფოსტო სისტემის სარეზერვო ასლების გაკეთება და შენახვა. სარეზერვო ასლების შენახვის პროცესი გულისხმობს არსებული მონაცემების კოპირებას, როგორიცაა მაგალითად წერილის შინაარსი და განკუთვნილია მხოლოდ ადმინისტრაციული მიზნებისათვის.
16. ელექტრონული ფოსტის, როგორც საკომუნიკაციო საშუალების გამოყენებისას, მომხმარებელი ვალდებულია იმოქმედოს ეთიკის კოდექსისა და უნივერსიტეტის შინაგანაწესი და დისციპლინური პასუხისმგებლობის ნორმებისა და უნივერსიტეტის ინფორმაციის დაცვის პოლიტიკის შესაბამისად. მომხმარებელი უნდა მოერიდოს ისეთი წერილების გაგზავნას, რომელიც მიმღებმა შეიძლება აღიქვას როგორც მიუღებელი და შეურაცხმყოფელი.

მუხლი 5. ანტივირუსის გამოყენება
1. ანტივირუსის გამოყენება ეხება უნივერსიტეტის ყველა საინფორმაციო ტექნოლოგიების საშუალებებს და მათ მომხმარებლებს.
2. ანტივირუსის გამოყენების მიზანია, მოხდეს უნივერსიტეტის კომპიუტერებისა და საინფორმაციო ტექნოლოგიების სისტემების კომპიუტერული ვირუსებით ინფიცირების თავიდან აცილება და სხვა გარე რისკებისაგან დაცვა. მისი გამოყენება მიზნად ისახავს უნივერსიტეტის საინფორმაციო ტექნოლოგიების აქტივების ძირითადი და ფართოდ გავრცელებული ვირუსებისაგან დაცვას.
3. მავნე პროგრამებისგან დაცვა უნდა ეფუძნებოდეს უსაფრთხოების შესახებ მომხმარებლის ცნობიერებას, შესაბამის სისტემებთან წვდომის და ცვლილების მართვის კონტროლს. კერძოდ:
ა) ვირუსების მაძიებელი და მკურნალი პროგრამული უზრუნველყოფის ინსტალაცია და რეგულარული განახლება კომპიუტერების და მედია მატარებლების სკანირების მიზნით, კონკრეტულ შემთხვევაში თუ რუტინული ფორმით;
ბ) გამოყენებამდე ელექტრონულ მატარებლებზე ნებისმიერი საეჭვო ან არა სანქციონირებული წარმოშობის ფაილის ან არასანდო ქსელის მეშვეობით მიღებული ფაილების შემოწმება ვირუსებზე;
გ) გამოყენებამდე მავნე პროგრამების არსებობაზე ელექტრონულ ფოსტაზე მიმაგრებული ფაილების და ჩატვირთული მასალის შემოწმება;
დ) ვირუსების განსაკუთრებით ადვილად გადამცემი არხების დაბლოკვა/გათიშვა კლიენტის მოწყობილობაზე (როგორებიცაა: დისკეტა, CD/DVD, USB და სხვა მატარებლები).

მუხლი 6. ანტივირუსის მართვა

1. უნივერსიტეტის კორპორატიულ ქსელთან ან ქსელურ წყაროებთან მიერთებამდე ან უშუალოდ მიერთების დროს ყველა საინფორმაციო ტექნოლოგიების საშუალებები (კომპიუტერები და სერვერები) აღჭურვილი უნდა იყოს სათანადოდ დაინსტალირებული, კონფიგურირებული, განახლებული და გაშვებული უნივერსიტეტის ანტი ვირუსის პროგრამით.

2. თუ კომპიუტერს უნივერსიტეტის ანტი ვირუსის პროგრამა არ გააჩნია, ის დაუყონებლივ უნდა დაინსტალირდეს. ამ წესთან დაკავშირებული ნებისმიერი გამონაკლისი უნდა შეთანხმებული იქნას საინფორმაციო ტექნოლოგიებისა დეპარტამენტის უფროსთან.

3. ანტი ვირუსის წესი შეიცავს მიმდინარე და შესაძლო საფრთხის, ინფიცირების რისკის ქვეშ მყოფ კომპიუტერების და სისტემების, ინფიცირებული კომპიუტერებისა და ფაილების იდენტიფიკაციის რეკომენდაციებს. ინფექციის შაბლონური ტიპები უნდა გამოვლინდეს და ქრონიკული შიდა და გარე საფრთხის გამოსავლენად გაუკეთდეს ანალიზი.

4. ვირუსების უმრავლესობა საფრთხეს წარმოადგენს სხვა კომპიუტერებისთვის, საერთო ინფიცირებული ქსელით სარგებლობის შემთხვევაში. ინფიცირებული კომპიუტერები დაუყონებლივ უნდა გაიწმინდოს ვირუსული ინფექციისგან. გაწმენდას დაქვემდებარებულ ფაილებს უნდა მოეხსნას ინფიცირებული კოდი და დაუბრუნდეს თავდაპირველ მდებარეობას. ის ფაილები, რომლებიც არ ექვემდებარება გაწმენდას, უნდა დარჩეს კარანტინში იმ დრომდე, სანამ მათი შეცვლა არა ინფიცირებული ასლებით იქნება შესაძლებელი. თუ ინფექციასთან ბრძოლის ყველა ხერხი უშედეგო აღმოჩნდა, საჭიროა კომპიუტერების მყარი დისკების დაფორმატება, ხოლო ყველა პროგრამა თავიდან უნდა დაინსტალირდეს არაინფიცირებული, ლიცენზირებული ასლების გამოყენებით. თუ ითვლება, რომ ინფიცირებულ კომპიუტერს შეუძლია ყველა სხვა კომპიუტერის ან ქსელის ინფიცირება, ინფიცირებული კომპიუტერი უნდა გამოირთოს ქსელიდან იმ დრომდე, სანამ ვირუსების არ არსებობა იქნება გარანტირებული.

მუხლი 7. ანტივირუსის ადმინისტრირება

1. ანტი ვირუსებთან დაკავშირებული საქმიანობის მართვა ცენტრალიზებულად ხორციელდება. ახალი ვირუსები მუდმივ საფრთხეს წარმოადგენს და მოითხოვს მუდმივად კვლევას მათ წინააღმდეგ ზომების დაგეგმვის უზრუნველსაყოფად. ახალი ვირუსის გამოვლენისთანავე, საჭიროა მომხმარებლების გაფრთხილება ახალი საშიშროების შესახებ.

2. ერთიანი ანტი ვირუსის პროგრამა გამოიყენება უნივერსიტეტის ყველა საინფორმაციო ტექნოლოგიების სისტემისთვის და კომპიუტერებისთვის. იგი ლიცენზირებულია და ლიცენზიის გახანგრძლივება ხდება ყოველწლიურად. ანტივირუსის განახლება კომპიუტერების შემთხვევაში ხორციელდება რეგულარულად, განრიგის შესაბამისად ინტერნეტით ან ავტომატურად სისტემური ადმინისტრატორის მიერ, რომელიც პასუხს აგებს ანტი ვირუსების ადმინისტრირებაზე. ყველა სერვერი და კომპიუტერი ავტომატურ რეჟიმში განახლებას ექვემდებარება.

3. ანტივირუსის სერვერი უზრუნველყოფს მომხმარებლების კომპიუტერების ყოველკვირეულ სკანირებას ვირუსებზე და აწარმოებს რეპორტინგს.

4. ინფიცირებული კომპიუტერები, თუ მათი გაწმენდა ავტომატურად არ ხერხდება, ხელით იწმინდება უნივერსიტეტის IT-დეპარტამენტის მომხმარებელთა მხარდაჭერის განყოფილების თანამშრომელთა მიერ.
5. მობილური კომპიუტერების მომხმარებლებს ორი შესაძლებლობა გააჩნიათ. თუ მობილური მომხმარებელი დომეინზეა დარეგისტრირებული, ანტი ვირუსის პროგრამა ცდილობს ანტივირუსის პროგრამის განახლებას კორპორატიული ქსელის მეშვეობით ცენტრალური კორპორატიული მონაცემთა ბაზიდან. თუ ამგვარი დაკავშირების

საშუალება არ არსებობს, განახლება კლიენტის პროგრამას უშუალოდ ანტი ვირუსის საიტიდან ინტერნეტის მეშვეობით უნდა შეეძლოს. ამგვარი შესაძლებლობა ავტომატურად უნდა იყოს შესაძლებელი კლიენტის პროგრამის კონფიგურაციის პარამეტრებში შესაბამისი ფუნქციების გააქტიურებით.
6. *.exe, *.bat, *.pif, *.scr, *.vba და სხვა სახის გაფართოებით ფაილების ჩამოტვირთვა და მიღება ელექტრონულ ფოსტით ან ქსელის მეშვეობით მთლიანი კორპორატიული ქსელისთვის აკრძალულია.
მუხლი 8. პასუხისმგებელი მხარეები
1. ანტივირუსის წესის დანერგვაზე და გამოყენებაზე პასუხს აგებენ ქსელისა და სერვერული სისტემების განყოფილებისა და ტექნიკური მხარდაჭერის განყოფილებების თანამშრომლები.
2. ზემოთ ჩამოთვლილი განყოფილების თანამშრომლები უნივერსიტეტის მასშტაბით არიან პასუხისმგებლები ყველა კომპიუტერზე (პერსონალური, პორტატიული კომპიუტერები, სერვერები) ანტი ვირუსის პროგრამული უზრუნველყოფის რეგულარულ განახლებაზე, აგრეთვე დროის გარკვეულ მონაკვეთებში შერჩეულ კომპიუტერებზე ანტი ვირუსის პროგრამული უზრუნველყოფის შემოწმებასა და მის განახლებაზე. თანამშრომლები ვალდებულნი არიან დარწმუნდნენ, რომ უნივერსიტეტის ყველა კომპიუტერი აღჭურვილია კორპორატიული ანტი ვირუსის პროგრამული უზრუნველყოფით. ამგვარი კონტროლი ხორციელდება ყოველკვირეულად და ითვალისწინებს მინიმუმ 2 შემთხვევით შერჩეული კომპიუტერების შემოწმებას, ხოლო მთლიანი უნივერსიტეტის საინფორმაციო სივრცის სკანირება (შემოწმება) ხორციელდება კვარტალში ერთხელ.