საჯარო სამართლის იურიდიული პირი –
ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი

ბრძანება №01-02/39

ქ. ბათუმი 31 მარტი 2020 წ.

საგანგებო მდგომარეობის მოქმედების პერიოდში ბსუ-ში სასწავლო პროცესის განხორციელების დამატებითი ღონისძიებების შესახებ

„უმაღლესი განათლების შესახებ“ საქართველოს კანონის 22-ე მუხლის, „განათლების ხარისხის განვითარების შესახებ“ საქართველოს კანონის, ბსუ-ს წესდების მე-13 მუხლის, ბსუ-ს აკადემიური საბჭოს 2015 წლის 08 ოქტომბრის №111 დადგენილებით დამტკიცებული „სასწავლო პროცესის მარეგულირებელი წესის“, ბსუ-ს აკადემიური საბჭოს 2018 წლის 20 თებერვლის №23 დადგენილებით დამტკიცებული „გამოცდების ჩატარების ინსტრუქციის“ საფუძველზე, ,,ახალ კორონავირუსთან დაკავშირებით პრევენციულ ღონისძიებათა განხორციელების წესის დამტკიცების შესახებ" საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის მინისტრის 2020 წლის 27 თებერვლის №296 ბრძანების, ,,ქვეყანაში კორონავირუსის გავრცელების თავიდან აცილების მიზნით პრევენციული ღონისძიებების განხორციელების შესახებ" საქართველოს მთავრობის 2020 წლის 02 მარტის №434 განკარგულების, კორონავირუსული ინფექციების შესაძლო გავრცელების აღკვეთის მიზნით ბსუ-ს პერსონალის სამსახურში გამოცხადებასთან დაკავშირებით გასატარებელ ღონისძიებათა შესახებ" ბსუ-ს ადმინისტრაციის ხელმძღვანელის 2020 წლის 13 მარტის N01-10/37 ბრძანების, ,ბსუ-ში 2019-2020 სასწავლო წელს გაზაფხულის სემესტრის სასწავლო პროცესის ორგანიზებულად ჩატარებისათვის გასატარებელი დროებითი ღონისძიებების შესახებ“ ბსუ-ს რექტორის 2020 წლის 16 მარტის №01-02/35 ბრძანების, ,,საქართველოში ახალი კორონავირუსის გავრცელების აღკვეთის მიზნით გასატარებელი ღონისძიების დამტკიცების შესახებ“ საქართველოს მთავრობის 2020 წლის 23 მარტის N181 დადგენილების, ,,საგანგებო მდგომარეობის მოქმედების პერიოდში საგანმანათლებლო დაწესებულებებში სასწავლო პროცესის განხორციელების შესახებ“ **საქართველოს მთავრობის 2020 წლის 31 მარტის N205 დადგენილებისა და სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციების** (MES 520 00322223, 31.03. 2020) საფუძველზე

ვ ბ რ ძ ა ნ ე ბ:

1. ,,საგანგებო მდგომარეობის მოქმედების პერიოდში საგანმანათლებლო დაწესებულებებში სასწავლო პროცესის განხორციელების შესახებ“ საქართველოს მთავრობის 2020 წლის 31 მარტის N205 დადგენილების საფუძველზე ბსუ-ში გატარდეს შემდეგი **დამატებითი ღონისძიებები:**

1.1. გაგრძელდეს „ბსუ-ში 2019-2020 სასწავლო წელს გაზაფხულის სემესტრის სასწავლო პროცესის ორგანიზებულად ჩატარებისათვის გასატარებელი დროებითი ღონისძიებების შესახებ“ ბსუ-ს რექტორის 2020 წლის 16 მარტის №01-02/35 ბრძანებით გათვალისწინებული ღონისძიებების, მათ შორის 2019-2020 სასწავლო წლის გაზაფხულის სემესტრის სასწავლო პროცესის წარმართვა დისტანციურად, ონლაინ სწავლების პლატფორმის (პროგრამის) „ZOOM" (შემდეგში „ზუმის“) მეშვეობით;

1.2. დისტანციური სწავლების განსახორციელებლად **სასწავლო პროცესის განმახორციელებელმა პერსონალმა** (შემდეგში „პროფესორ-მასწავლებლებმა“):

ა) გააგრძელონ ბსუ-ს სტუდენტური პორტალის (portal.bsu.edu.ge) ელექტრონული ველის **„ელ.სწავლება“** გამოყენება და იხელმძღვანელონ ამავე პორტალზე განთავსებული და შესაბამისი ფაკულტეტის დეკანის მიერ მიწოდებული ინსტრუქციით, ასევე საქართველოს სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციებით **(წინამდებარე ბრძანების დანართი 1);**

ბ) სასწავლო პროცესის დისტანციური საშუალებებით წარმართვისას იხელმძღვანელონ ევროპის უმაღლესი განათლების ხარისხის უზრუნველყოფის სააგენტოების ასოციაციის (ENQA) მიერ 2018 წელს შემუშავებული ელექტრონული სწავლების შიდა ხარისხის უზრუნველყოფის სახელმძღვანელო პრინციპებით;

გ) საგანგებო მდგომარეობის ვადის გასვლის შემდეგ ბსუ-ს შესაბამისი ფაკულტეტის დეკანთან და ხარისხის უზრუნველყოფის სამსახურის უფროსთან ერთად განიხილონ საკითხი დისტანციური სწავლების მიღმა დარჩენილი სტუდენტებისათვის უმაღლესი განათლების სრულად ხელმისაწვდომობისათვის შესარჩევი ფორმების შესახებ.

1.3. „ზუმი“-ს პროგრამის გამოყენების პროცესის კოორდინაცია განახორციელოს სტუდენტთა კარიერული განვითარების, კულტურისა და სპორტის დეპარტამენტის უფროსმა (მ. დიასამიძე), ამავე დეპარტამენტის სტუდენტთა ელექტრონული სერვისების განყოფილების უფროსმა (ა. შარაძე) და საინფორმაციო ტექნოლოგიების სამსახურმა (ზ. ბერაძე);

1.4. **რექტორის მოადგილემ (თ. სირაძე)** და უნივერსიტეტის **ხარისხის უზრუნველყოფის სამსახურის ხელმძღვანელის მოვალეობის შემსრულებელმა (ი. კორძაია)** წინამდებარე ბრძანების გამოცემიდან 3 სამუშაო დღეში ერთობლივად უზრუნველყონ საქართველოს მთავრობის 2020 წლის 31 მარტის N205 დადგენილების მე-2 მუხლის მე-6 პუნქტით გათვალისწინებული წერილის *(სასწავლო პროცესის დისტანციურად განხორციელების, კურიკულუმის დაგეგმვის, სასწავლო პროცესის ორგანიზებისა და ადმინისტრირებისათვის საჭირო მიდგომებისა და მეთოდების გამოყენების თაობაზე)* მომზადება სსიპ - განათლების ხარისხის განვითარების ეროვნული ცენტრისათვის **არაუგვიანეს 2020 წლის 4 აპრილისა** წარდგენისათვის;

1.5. **ბსუ-ს კოლეგიური ორგანოების** (აკადემიური საბჭო, წარმომადგენლობითი საბჭო, ფაკულტეტის საბჭო, სადისერტაციო საბჭო) **სხდომები** გაიმართოს (ასეთის

საჭიროების შემთხვევაში) დისტანციურად, საქართველოს კანონმდებლობისა და ამ ორგანოების რეგლამენტების/დებულებების მოთხოვნათა გათვალისწინებით (მათ გამართვის შესახებ შესაბამისი ორგანოს სამდივნომ/მდივანმა უზრუნველყონ ტექნიკური დახმარების საჭიროების განსაზღვრა და შესაბამისი სამსახურებრივი ბარათის წარმოდგენა);

1.6. **ბსუ-ში დასაქმებული ყველა პირი გადაყვანილი იქნეს დისტანციური მუშაობის რეჟიმზე,** გარდა იმ შემთხვევისა, როდესაც კონკრეტული პოზიციის/თანამდებობის პირის უმაღლესი საგანმანათლებლო დაწესებულების ტერიტორიაზე ყოფნა/გამოცხადება დაკავშირებულია ამ პოზიციის/თანამდებობის სპეციფიკაციასთან. ამ პირების საქმიანობა განხორციელდეს საქართველოს მთავრობისა და ბსუ-ს ტერიტორიაზე დაშვებული იქნეს შესაბამისი სტრუქტურული ერთეულების უფროსების მიერ განსაზღვრულ, კრიტიკულად მნიშვნელოვანი აუცილებლობის შემთხვევებში და მხოლოდ საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს მიერ გაცემული რეკომენდაციების გათვალისწინებით.

2. წინამდებარე ბრძანების 1.1. – 1.4. პუნქტების აღსრულების კონტროლი განახორციელოს რექტორის მოადგილემ (თ. სირაძე) და ხარისხის უზრუნველყოფის სამსახურის ხელმძღვანელის მოვალეობის შემსრულებელმა (ი. კორძაია).
3. წინამდებარე ბრძანების 1.5.- 1.6. პუნქტების აღსრულებაზე კონტროლი განახორციელონ რექტორმა და ადმინისტრაციის ხელმძღვანელმა.
4. ბრძანება განთავსდეს ბსუ-ს ვებგვერდზე.
5. ბრძანება ძალაშია ხელმოწერისთანავე.
6. ბრძანება გასაცნობად და აღსასრულებლად დაეგზავნოს ბსუ-ს ფაკულტეტებს, ყველა სტრუქტურულ ერთეულს და დასაქმებულს.

რექტორი, ასოცირებული პროფესორი **მერაბ ხალვაში**

,,საგანგებო მდგომარეობის მოქმედების პერიოდში ბსუ-ში სასწავლო
პროცესის განხორციელების დამატებითი ღონისძიებების შესახებ“
ბსუ-ს რექტორის 2020 წლის 31 მარტის N 01-02/39 ბრძანების

დანართი 1

სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები

COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება

მონაცემთა დაცვის კანონმდებლობა პანდემიის ან სხვა რაიმე საგანგებო სიტუაციის დროს არ აბრკოლებს აუცილებელი ინფორმაციის გაზიარების პროცესს, თუმცა არანაკლებ მნიშვნელოვანია, როგორც ჯანმრთელობის დაცვაზე პასუხისმგებელმა უწყებებმა, ასევე, საჯარო და კერძო დამსაქმებლებმა იცოდნენ თუ როგორ და რა დოზით შეიძლება პერსონალური, მათ შორის, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გაზიარება.

ჯანდაცვის დაწესებულებების მიერ მონაცემთა დამუშავება

საზოგადოებრივი ჯანდაცვის დაწესებულებები, მოქმედი კანონმდებლობის საფუძველზე, აგროვებენ და ამუშავებენ სხვადასხვა პერსონალურ მონაცემებს, რაც აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისა და ფუნქციონირებისთვის.

ვირუსის გავრცელების წინააღმდეგ ბრძოლის პროცესში, ჯანდაცვის დაწესებულებებს უწევთ ინფიცირებულ ან/და შესაძლო ინფიცირებულ პირთა შესახებ მეტი მოცულობით მონაცემების შეგროვება, ვიდრე სტანდარტულ შემთხვევებში (მაგალითად, აგროვებენ ინფორმაციას მოქალაქეთა საზღვარგარეთ მოგზაურობის, სამუშაო ადგილის, ახლო კონტაქტში მყოფი პირების შესახებ), რაც არსებული საჭიროებიდან გამომდინარეობს და არ ეწინააღმდეგება კანონმდებლობას.

პანდემიის შესახებ საზოგადოების ინფორმირებისა და სამედიცინო კონსულტაციების გაწევის მიზნით, დასაშვებია საინფორმაციო შეტყობინებების გაგზავნა სატელეკომუნიკაციო და თანამედროვე ტექნოლოგიების საშუალებით.

გასათვალისწინებელია, რომ ასეთი სიტუაციების დროს, იზრდება შეცდომაში შემყვანი და ე. წ. ,,თაღლითური შეტყობინებების“ მიღების რისკი. შესაბამისად, მნიშვნელოვანია, მოქალაქეები დაეყრდნონ მხოლოდ ოფიციალური ორგანოებიდან მიღებულ ინფორმაციას.

ვირუსით ინფიცირებულ, შესაძლო ინფიცირებულ ან/და მათთან კონტაქტში მყოფ პირთა ვინაობის (სახელის, გვარის) საჯაროდ გავრცელება, როგორც წესი, აუცილებელი არ არის და საზოგადოებრივი ინტერესის დასაკმაყოფილებლად საკმარისია მათ შესახებ არაიდენტიფიცირებადი ფორმით ინფორმაციის გავრცელება (მოქალაქეობა, ეთნიკური კუთვნილება, ასაკი, სამუშაო ადგილი, მათი გადაადგილების მარშრუტი და ა.შ.). აღნიშნულ

პირთა ვინაობის შესახებ მონაცემების გასაჯაროება და მესამე პირთათვის გამჟღავნება დასაშვებია იმ მოცულობითა და იმ ფარგლებში, რაც აუცილებელია დაავადების პრევენციის, კონტროლისა და მართვისათვის.

დამსაქმებელი ორგანიზაციების მიერ დასაქმებულთა მონაცემების დამუშავება

დასაქმებულთათვის უსაფრთხო გარემოს უზრუნველყოფის პარალელურად, დამსაქმებლები ცდილობენ შეინარჩუნონ საქმიანობის უწყვეტობა.

კანონმდებლობის თანახმად, დამსაქმებლებს დასაქმებულთა დაინფიცირების შესახებ ინფორმაციის შეგროვება შეუძლიათ დასაქმებულთა ნების მიუხედავად, თუ ეს ემსახურება უსაფრთხო შრომითი გარემოს უზრუნველყოფას ან/და ემსახურება ჯანმრთელობის დაცვის სისტემის მართვას.

დასაშვებია დამსაქმებელმა შეაგროვოს შემდეგი ინფორმაცია: დასაქმებული სტუმრობდა თუ არა ვირუსის გავრცელების მაღალ რისკის შემცველ ქვეყანას, აქვს თუ არა დასაქმებულს ვირუსის სიმპტომები, ჰქონდა თუ არა კონტაქტი ვირუსით დაინფიცირებულ პირ(ებ)თან.

დასაქმებულის დაინფიცირების შესახებ ეჭვის შემთხვევაში დამსაქმებელმა უნდა მიმართოს შესაბამის ჯანდაცვის უწყებას და დაექვემდებაროს მის მითითებებს.

დამსაქმებლის მიერ, დასაქმებულის დაინფიცირების შესახებ, ინფორმაციის სხვა დასაქმებულებისათვის გამჟღავნება დასაშვებია, თუ ეს აუცილებელია დასაქმებულთან კონტაქტში მყოფი პირების გამოსავლენად ან/და ვირუსის შემდგომი გავრცელების პრევენციისთვის.

მოპოვებული მონაცემები დამსაქმებელმა უნდა შეინახოს იმ ვადით, რაც აუცილებელია მის კომპეტენციას მიკუთვნებული ღონისძიებების განხორციელებისთვის. შემდგომ ეს მონაცემები უნდა წაიშალოს, განადგურდეს ან შენახულ იქნას პირის იდენტიფიცირების გამომრიცხავი ფორმით.

დისტანციური სწავლება და შეხვედრები

დისტანციურ სწავლებაზე გადავიდნენ საგანმანათლებლო დაწესებულებებიც (სკოლები, უნივერსიტეტები), ასევე ხშირია დისტანციურად შეხვედრების გამართვის პრეცედენტები.

სოციალურ ქსელებში ვრცელდება ონლაინ სასწავლო პროცესის, ონლაინ შეხვედრების ამსახველი (მათ შორის, იუმორისტული) ფოტო-ვიდეო მასალა.

ონლაინ შეხვედრების, ონლაინ-სწავლების ამსახველი მასალა (ფოტო, ვიდეო გამოსახულება) წარმოადგენს პირის პერსონალურ მონაცემებს, რაც უნდა იქნეს გათვალისწინებული მათი გასაჯაროებისას.

არასრულწლოვნის მონაცემების ინტერნეტში ყველასთვის ხელმისაწვდომი ფორმით გასაჯაროებამ შესაძლოა არასასურველი ზეგავლენა მოახდინოს არასრულწლოვანზე (გახდეს ბულინგის ან სხვა სახის არასასურველი მოპყრობის ობიექტი).

შესაბამისად, საგანმანათლებლო დაწესებულებები, ამ დაწესებულებებში დასაქმებული პირები, ასევე, არასრულწლოვანი პირების მშობლები და ოჯახის წევრები, მეტი

პასუხისმგებლობით უნდა მოეკიდონ ბავშვების მონაცემების გასაჯაროებას და იმოქმედონ არასრულწლოვნის საუკეთესო ინტერესების გათვალისწინებით.

დისტანციური შეხვედრებისათვის გამართვისათვის, შეგიძლიათ გამოიყენოთ თანამედროვე კოლაბორაციული კომუნიკაციის სისტემები (მაგალითად, Webex, Zoom, Teams და ა.შ.).

დისტანციურად მუშაობისას მონაცემთა დამუშავება

ორგანიზაციათა უმეტესობამ უკვე მიმართა დისტანციურად მუშაობის რეჟიმს. თანამედროვე ტექნოლოგიებმა დისტანციურად მუშაობა მარტივი გახადა, თუმცა ასეთ დროს დღის წესრიგში დგება სამსახურებრივი ინფორმაციის კონფიდენციალობის დაცვისა და უსაფრთხოების საკითხი.

დისტანციურად მუშაობისას გასათვალისწინებელი გარემოებები:

- ✓ სახლიდან დისტანციურად მუშაობისას სასურველია გამოყენებულ იქნეს სამსახურის კომპიუტერი;
- ✓ თუ საჭიროა სახლის კომპიუტერიდან სამსახურის კომპიუტერში დისტანციური წვდომის საშუალებებით შესვლა, ამისათვის აუცილებლად უნდა იქნეს გამოყენებული თანამედროვე და განახლებული პროგრამები;
- ✓ საკუთარ კომპიუტერში რეგულარულად უნდა განახლდეს ოპერაციული სისტემები (MS Windows, MacOS);
- ✓ აუცილებელია კომპიუტერში შესვლის პაროლის დაყენება;
- ✓ იმ ელექტრონულ სისტემებში შესვლისთვის, რომელზეც წვდომა ინდივიდუალური მომხმარებლის სახელით არის შესაძლებელი, უმჯობესია გამოყენებულ იქნეს რთული და კომპლექსური პაროლი (რომელიც შეიცავს არანაკლებ 10 სიმბოლოს, დიდ და პატარა ლათინურ ასოებს, ციფრებს და სპეციალურ სიმბოლოებს. მაგ.: #,$, &, @ და ა.შ.). ასევე, სადაც ეს შესაძლებელია, გამოყენებულ უნდა იქნეს ორ ფაქტორიანი ავთენტიფიკაციის მექანიზმები (მომხმარებლის სახელთან ერთად, პაროლი და დამატებითი ერთჯერად კოდი);
- ✓ ერთიდაიგივე პაროლი არ უნდა იქნეს გამოყენებული სხვადსხვა სისტემებში შესვლისათვის;
- ✓ სამსახურის შიდა ელექტრონულ რესურსებთან წვდომისათვის გამოყენებული უნდა იქნეს მხოლოდ დაშიფრული VPN კავშირის საშუალებები;
- ✓ გამოყენებული უნდა იქნეს ანტივირუსული პროგრამები, თუნდაც უფასო ვერსიები;
- ✓ სასურველია მონაცემების სარეზერვო ასლების გაკეთება ან მნიშვნელოვანი დოკუმენტების და მონაცემების სამსახურის სერვერზე შენახვა;
- ✓ უნდა დაიშიფროს კონფიდენციალური მონაცემები, თუნდაც უფასო შიფრაციის პროგრამების გამოყენებით (მაგალითად, VeraCrypt, BitLocker და ა.შ.);
- ✓ არ უნდა იქნეს გამოყენებული უცხო USB მონაცემთა მატარებლები;
- ✓ დაცული უნდა იქნას კომპიუტერის ფიზიკური უსაფრთხოება (დამსაქმებელმა იგი არ უნდა დატოვოს უყურადღებოდ სხვადასხვა ადგილზე).

ასევე, **დასაქმებულმა უნდა უზრუნველყოს** სახლის უკაბელო ქსელური მოწყობილობის უსაფრთხოება. კერძოდ:

- ✓ სახლის უკაბელო ქსელური მოწყობილობის მართვისათვის გამოყოფილი მომხმარებლის პაროლი არ უნდა იყოს სხვისთვის ცნობილი;
- ✓ შესაძლებლობის შემთხვევაში, უმჯობესია ინტერნეტიდან შეიზღუდოს უკაბელო ქსელური მოწყობილობის სამართავ პანელზე წვდომა;

- ✓ უკაბელო ქსელური კავშირისათვის გამოყენებული შიფრაციის მეთოდები სასურველია იყოს თანამდეროვე (მაგალითად, WPA2 ან WPA3);
- ✓ სახლის უკაბელო ქსელურ მოწყობილობასთან დაკავშირების პაროლი უნდა იყოს კომპლექსური და არანაკლებ 16 სიმბოლოსგან შემდგარი;
- ✓ პერიოდულად უნდა შეიცვალოს უკაბელო ქსელის მოწყობილობასთან დაკავშირების პაროლი.

დამატებით უნდა აღინიშნოს, რომ პანდემიით გამოწვეული ვითარებით სარგებლობენ ჰაკერები.

მსოფლიოში ბევრი ცრუ ე.წ. „ფიშინგ" საიტებია შექმნილი, სადაც განთავსებულია ვირუსის გავრცელების სტატისტიკური მონაცემები და რომლებზეც შესვლის შემდგომ შესაძლებელია კომპიუტერებიდან მონაცემების მოპარვა. შესაბამისად, რეკომენდებულია ვირუსის გავრცელების სტატისტიკური მონაცემების მხოლოდ ოფიციალურ ან საინფორმაციო სააგენტოებისა და მედია ორგანიზაციების საიტებზე დათვალიერება.

ასევე, ძალიან მომატებულია ელ-ფოსტით გაგზავნილი ცრუ ე.წ. „ფიშინგ" წერილების რაოდენობა. ამა თუ იმ ცნობილი ორგანიზაციის ან ადამიანის სახელით ცრუ შეტყობინებები იგზავნება კონფიდენციალური ან პერსონალური ინფორმაციის მოპარვის მიზნით.

საფრთხის შემცველია უცნობი ორგანიზაციების და პირების მიერ გამოგზავნილ წერილებში მიმაგრებული ფაილები. შესაბამისად, მიბმული ფაილები არ უნდა გაიხსნას, სანამ მომხმარებელი არ დარწმუნდება, გამომგზავნი ორგანიზაციის ან/და პირის კეთილსინდისიერებასა და რეალურობაში.