დამტკიცებულია აკადემიური საბჭოს მიერ
25.09.2020 №36

საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) უსაფრთხოების წესი
(პერსონალურ მონაცემთა დაცვის მექანიზმები)

ელექტრონული, დისტანციური, შერეული ტიპის სწავლების ფარგლებში აუცილებელია კიბერსივრცისა და საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) წესების დაცვა. ამ მიზნით სასწავლო უნივერსიტეტს შემუშავებული აქვს საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) უსაფრთხოების წესი „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და მონაცემთა დაცვის სააგენტოს სტანდატიზაციის გათვალისწინებით და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს.

სასწავლო უნივერსიტეტის კიბერსივრცე გულისხმობს ელექტრონული მოწყობილობებისა და (ელექტრომაგნიტური, არსებობის შემთხვევაში) სპექტრის გამოყენებას ქსელით დაკავშირებული სისტემებისა და დამხმარე ინფტრასტრუქტურის მეშვეობით მონაცემთა შენახვისთვის, შეცვლისთვის ან გაცვლისთვის.

რომ არ მოხდეს კიბერსივრცეზე შეტევა საგანმანათლებლო დანიშნულების ინფორმაციაზე, ადმინისტრაციულ სისტემებზე, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით, ამისთვის არსებობს საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) წესი.

ინფორმაციული უსაფრთხოება გულისხმობს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას.

სასწავლო უნივერსიტეტში ინფორმაციული უსაფრთხოების მართვის სისტემა არის მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია საგანმანათლებლო საქმიანობის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება.

საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) კიბერუსაფრთხოების მართვისა და კონტროლისთვის საჭიროა კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით.

სასწავლო უნივერსიტეტის IT მომსახურებაზე პასუხისმგებელმა პირებმა უნდა უზრუნველყონ ცნობიერების ამაღლების მიზნით განხორციელებული ტრენინგების საშუალებით რომ შესაბამისი პერსონალი აცნობიერებდეს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელობას და მათ მიერ ინფორმაციული უსაფრთხოების მიღწევაში შეტანილ წვლილს.

ინფორმაციული უსაფრთხოების მიზნებისთვის გამოიყენება „დაგეგმვა-აღსრულება-შემოწმება-ქმედება“ მოდელი, რაც უზრუნველყოფს საქმიანობის ხარისხს.

სასწავლო უნინვერსიტეტის უკაბელო ინტერნეტის საშუალებით პირადი მოწყობილობებიდან სტუდენტსა და სხვა ჩართულ პირებს ეძლევათ წვდომა ინტერნეტზე შენობის შიგნით და გარეთ გარკვეულ პერიმეტრსა და გარკვეული შეზღუდვების გათვალისწინებით (შეზღუდვები არ ეხება საგანმანათლებლო მიზნით გამოსაყენებელ ვებ გვერდებს).

იმდენად, რამდენადაც ნებისმიერი მოწყობილობა (აიფონი, ტაბლეტი, აიპადი, მობილური ტელეფონი, ლეპტოპი და სხვა), რომელიც გამოიყენება სასწავლო უნივერსიტეტის ინტერნეტ მომსახურებებთან წვდომისთვის, წარმოადგენს საფრთხეს უნივერსიტეტის ქსელური სისტემისთვის (ვირუსები და მავნე პროგრამები, განახლებადი პროგრამები და სხვა), უნივერსიტეტი იტვებს უფლებას გადაამოწმოს ინტერნეტთან წვდომისთვის გამოყენებული მოწყობილობები.

იმ შემთხვევაში თუ უნივერსიტეტის ქსელი დადგება საფრთხის წინაშე მისი მომხმარებლების მხრიდან სხვადასხვა სოციალური ქსელის (facebook, youtube, twitter, linkedin და სხვა) გამოყენების გამო, უნივერსიტეტი იტოვებს უფლებას დაბლოკოს აღნიშნული ქსელების მოხმარება თავისი სივრცის ფარგლებში.

ვირტუალიზაცია ფართოდ გამოიყენება ყველა ტიპის ორგანიზაციაში და მით უმეტეს ელექტრონულ სწავლებაში, რაც გულისხმობს მნიშვნელოვან დანაზოგს ტექნიკისა და მენეჯმენტის თვალსაზრისით. თუმცა აღნიშნული საფრთხეს უქმნის უნივერსიტეტის ქსელს, ამდენად ვირტუალიზაციის გადასინჯვაც უნდა მოხდეს იმავე პრინციპებით, როგორც ჩვეულებრივი მოწყობილობების.

IT consumerization (აიტი სამომხმარებლო მომსახურება) ხშირად ხდება ჩართული პირების პირადი მოწყობილობებითა და პირადი ონლაინ ექაუნთებით, ხშირად პირადი აპლიკაციებით უერთდებიან უნივერსიტეტის ქსელს ყოველგვარი ნერბართვის გამოთხოვის გარეშე. მსგავსი ქმედებები იწვევს ისეთ პრობლემებს, რომელთა მართვა ხშირად ურთულესია. აღნიშნული ხშირად მოითხოვს ინფტრასტრუქტურის განახლებასაც. აღნიშნული ფაქტის შემჩნევისას უნივერსიტეტი იტოვებს უფლებას აუკრძალოს მომხმარებელს აღნიშნული ქმედება იმ შემთხვევაში თუ ვერ უზრუნველყოფს უნივერსიტეტი მსგავსი ქმედებების იდენტიფიკაციას არსებული მოწყობილობითა და ინფტრასტრუქტურით.

ელექტრონული (ონლაინ, დისტანციური, შერეული ტიპის) სწავლება გულისხმობს იმავე გამოწვევებს, რასაც პირისპირ სწავლება. ისიც გულისხმობს ინფორმაციის გაზიარებასა და გავრცელებას. ამ შემთხვევაში ინტერაქცია გულისხმობს მომხმარებელთა, ქსელის, ინტერნეტის, მონაცემთა ბაზებისა და სხვა კომპონენტების ინტეგრაციას.

ონლაინ, დისტანციური, შერეული ტიპის სწავლება დაუცველია მთელი რიგი საფრთხეებისაგან (ვირუსები, მავნე პროგრამები და სხვა მსგავსი) როგორიცაა ჯაშუშობა, არალეგალურად ინფორმაციის ქურდობა, ინტელექტუალური ქრუდობა, ინფორმაციის უნებართვო ჩამოტვრითვა, ატვირთვა, აუთენტიფიკაცია, ხელმისაწვდომობა, კოფიდენციალურობის ხელყოფა, ინფორმაციის გაჟონვა, აკადემიური კეთილსინდისიერება და სხვა მსგავსი ქმედებები.

სასწავლო უნივერსიტეტი უწევს ორგანიზებას ტრენინგებს საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) უსაფრთხოების დაცვისა და აუცილებლობის შესახებ ცნობიერების ამაღლების მიზნით. თანაბარი გააზრება ყველა ჩართული მხარის მხრიდან კიბერუსაფრთხოების საფრთხეებისა და სარგებლის შესახებ, ყველა ჩართულ პირს დაეხმარება მის დაცვაში.

საგანმანათლებლო სივრცის ციფრული (კიბერუსაფრთხოების) უსაფრთხოების მიზნით გამოყოფენ შემდეგი ტიპის საფრთხეებს:

მიზანმიმართული პროგრამული შეტევა (სხვადასხვა ვირუსებითა და მავნე პროგრამებით)

ტექნიკური პროგრამული უზრუნველყოფის ხარვეზები და შეცდომები (კოდირების პრობლემები, უცნობი ხარვეზები)

ადამიანური შეცდომებისა და მოქმედებების შედეგები (უბედური შემთხვევები, თანამშრომელთა შეცდომები)

ჯაშუშობა ან განზრახ დანაშაულებრივი ქმედებები (არასანქცირებული წვდომა, ან/და მონაცემთა შეგროვება)

დივერსიული ან ვანდალიზმის ქმედებები (ინფორმაციის ან სისტემის განადგურება)

ტექნიკის ხარვეზი ან ჩავარდნა

მიზანმიმართული ქურდობა (ტექნიკის ან ინფორმაციის უკანონო კონფისკაცია)

აკადემიური კეთილსინდისიერება (პლაგიატი, საავტორო უფლებების რღვევა)

მომსახურების მიწოდების ხარისხი მიმწოდებლისგან

ტექნოლოგიური სიბერე (მოძველებული აპარატურა)

ინფორმაციის გამოძალვა (შანტაჟი ინფორმაციის გამჟღავნების მიზნით)

წარმოდგენილია სასწავლო უნივერსიტეტის უსაფრთხოებსი რისკები და მათგან თავდაცვის მექანიზმები

უსაფრთხოების რისკები	თავდაცვის მექანიზმები
ARP cache poisoning and MITM attack • Brute force attack • Cross-Site Request Forgery (CSRF) • Cross Site Scripting (XSS) • Denial of Service (DoS) • IP spoofing • Masquerade • Rootkits • SQL Injection • Session Hijacking • Session Prediction • Stack-smashing attacks	• Installing firewalls and anti-virus software • Implementing Security Management (ISM) • Improving authentication, authorisation, confidentiality, and accountability • Using digital right management and cryptography • Training security professionals

კიბერ უსაფრთხოება ყველა ჩართული პირის პასუხისმგებლობაა დაწყებული მართვის ორგანოებიდან აკადემიური და ადმინისტრაციული პერსონალი, დახმარე პერსონალი და ყველა მომხმარებელი.

ლექციების აუდიო/ვიდეოჩანაწერები და ონლაინ სასწავლო შეხვედრების ამსახველი ვიდეო/აუდიო/ფოტომასალა, მათ შორის, ე.წ. „სქრინშოთი", წარმოადგენს პერსონალურ მონაცემს და ეს გათვალისწინებული უნდა იყოს როგორც სტუდენტების, პროფესიული სტუდენტების ასევე აკადემიური პერსონალის/პროფესიული განთლების მასწავლებლების მიერ მათი მოსმენისას და შენახვისას.

სტუდენტებთან/პროფესიულ სტუდენტებთან კომუნიკაცია განხორციელდეს მათი საჭიროებების გათვალისწინებითა და მათი პირადი სივრცის პატივისცემის პრინციპის დაცვით, რადგან ელექტრონული (ონლაინ) სწავლებისას განსაკუთრებით მნიშვნელოვანი ხდება პერსონალურ მონაცემთა დაცვის საკითხი.

სასწავლო უნივერსიტეტის სოციალურ მეცნიერებათა და ჯანდაცვის ფაკულტეტის საგანმანათლებლო პროგრამების განმახორციელებელი აკადემიური და მოწვეული პერსონალის, პროფესიული საგანმანათლებლო პროგრამების განმახორციელებელი პროფესიული განათლების მასწავლებლების მიერ საგანგებო ვითარებაში საკუთარი სტუდენტებისათვის/პროფესიული

სტუდენტებისთვის ელექტრონული ფორმატით მომზადებული სალექციო მასალები (ვიდეო/აუდიოლექციები, სალექციო პრეზენტაციები და სხვ.) გამოყენებულ უნდა იქნეს მხოლოდ ამ საგანმანათლებლო პროგრამების სასწავლო კურსებზე რეგისტრირებულ სტუდენტთა/პროფესიულ სტუდენტთა მიერ და მხოლოდ სასწავლო მიზნებისათვის, დანიშნულებისამებრ, დაუშვებელია მათი გაზიარება არაუფლებამოსილი მესამე პირებისათვის და მათი საჯაროდ ხელმისაწვდომად ქცევა, მათ შორის, სოციალური ქსელების მეშვეობით სხვადასხვა ჯგუფებში.

ყველა ასეთი შემთხვევით შესაძლოა შეიქმნას „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის დარღვევის პრეცედენტი.

უნივერსიტეტისგან ჩართული პირებისთვის G-suit -ზე არსებული ანგარიშების (google) უსაფრთხოების მიზნით შემუშვებულია რეკომენდაციები:

1. სტუდენტური ელექტრონული ფოსტის პაროლი აუცილებელია იყოს მინიმუმ 8 (რვა) სიმბოლო
2. რეკომენდირებულია რთული პაროლი. სირთულისთვის საჭიროა კოდური სიტყვა შეიცავდეს სიმბოლოს, რიცხვს, ლათინურ „Uppercase“ და „Lowercase” ასოებს (მაგ : Mm; Dd; Aa).
3. რეკომენდირებული არ არის ელ-ფოსტის მისამართში არსებული სიტყვის გამოყენება პაროლად.
4. რეკომენდირებულია ტელეფონის ნომრის მიმაგრება სტუდენტურ ანგარიშზე.
5. ვინაიდან უნივერსიტეტი იყენებს G suite-ს, ასევე რეკომენდირებულია ანგარიშზე - „ორმაგი ავთენტიფიკაციის“ ჩართვა. მაგ : Google Authenticator აპლიკაცია.
6. არ არის რეკომენდირებული უცნობ კომპიუტერულ მოწყობილობაზე ავტორიზაცია. *(შესაძლებელია მავნე პროგრამებით თქვენი მონაცემების მითვისება)*
7. ნებისმიერი სხვა მოწყობილობის გამოყენების შემთხვევაში აუცილებლად გადით სისტემიდან.
8. ანგარიშის მომხმარებლის სახელი და პაროლი არ შეინახოთ ავტორიზაციის დროს.
9. უნებურად შენახვის შემთხვევაში გაასუფთავეთ Browser-ის ისტორია. (*ან გამოიყენეთ Incognito, Private რეჟიმი, რომელიც არ ინახავს თქვენს ციფრულ ისტორიას კომპიუტერის მესხიერებაში)*
10. პერიოდულად ცვალეთ პაროლი და გადაამოწმეთ თქვენი ანგარიშის აქტიური სესიები.