ინფორმაციული უსაფრთხოების პოლიტიკა (მაღალი დონე)

საქართველოს უნივერსიტეტის კორექტული და ეფექტიანი ფუნქციონირებისათვის ინფორმაციის მთლიანობა, კონფიდენციალობა და ხელმისაწვდომობა არის ძალიან მნიშვნელოვანი.

მარცხმა ამ სფეროში შესაძლებელია გამოიწვიოს უნივერსიტეტის მიერ მიწოდებული მომსახურების კრახი და არსებულ თუ პოტენციალურ პარტნიორებსა და კლიენტებში კომპანიის ნდობის დაკარგვა. ამიტომ ჩვენი კომპანიის წარმატებული ფუნქციონირებისათვის ჩვენი ინფორმაციის და აქტივების უსაფრთხოება შეფასებულია, როგორც ფუნდამენტალური მნიშვნელობის.

წინამდებარე პოლიტიკა ვრცელდება:

- კომპანიის ყველა პერსონალსა და ვიზიტორზე
- კომპანიის საკუთრებაში მყოფ ან მართულ ინფორმაციულ აქტივებზე
- ინფორმაციასთან დაშვების უფლებასა და კონტროლზე
- ინფორმაციული სისტემების და სერვისების უსაფრთხოებაზე
- ბიზნესის განგრძობადობასა და ინფორმაციის კატასტროფის აღდგენაზე
- მარეგულირებელი და სამართლებრივი მოთხოვნების შესრულების სათანადო კონტროლზე
- მესამე მხარეებისა და კომპანიის პერსონალისათვის დადგენილი პროცედურების დაცვაზე
- ინფორმაციული უსაფრთხოების მიმართ ხელმძღვანელობის მხარდაჭერასა და რჩევაზე
- ინფორმაციული უსაფრთხოების დარღვევის აღმოფხვრის პროცესებზე.

ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს ბიზნესის განგრძობადობას და ბიზნესის დაზიანების მინიმიზირებას ინფორმაციული უსაფრთხოების ინციდენტების პრევენციით და მართვით ბიზნესზე გავლენის მისაღებ დონემდე.

წინამდებარე პოლიტიკის შესრულება გვეხმარება დავიცვათ ჩვენი კომპანია, ჩვენი პერსონალი, სტუდენტები შიდა, თუ გარე, შეგნებული, თუ უნებლიე ინფორმაციული საფრთხეებისაგან. ჩვენ მზად ვართ დაინტერესებული მხარეების კარგი საინფორმაციო უსაფრთხოების უზრუნველყოფისათვის.

წინამდებარე პოლიტიკის მიზნები მიიღწევა ჩვენი ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებით, რომელიც მოიცავს ISO 27001-ის მიხედვით შემუშავებულ უსაფრთხოების სტანდარტებს, პროცედურებს და სახელმძღვანელოებს.

უნივერსიტეტის ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს, რომ:

- ინფორმაცია ხელმისაწვდომია მხოლოდ უფლებამოსილი პირისთვის, ვისაც აქვს დაშვება
- დაცულია ინფორმაციის სისწორე, სისრულე და დამუშავების მეთოდები

ინფორმაციული უსაფრთხოების პოლიტიკა (მაღალი დონე)

- ყველა საჭირო შემთხვევაში ავტორიზებულ პირებს აქვთ ხელმისაწვდომობა ინფორმაციასთან და მასთან დაკავშირებულ აქტივებთან
- ინფორმაცია არის უსაფრთხოდ დაცული ამ ინფორმაციის კონფიდენციალობის დარღვევის, არასაკმარისი მთლიანობის ან ხელმისაწვდომობის შეფერხების შედეგებისაგან
- განსაზღვრულია ინფორმაციის კლასიფიკაციის სქემა კლასების აღწერით და კონკრეტული კლასის ინფორმაციის მართვის წესი (შენახვა, შემოწმება, გადაგზავნა, გაზიარება და განადგურება)
- ინფორმაციის უსაფრთხოების ყველა მოთხოვნა სრულდება შესაბამისი რეგულაციების, კანონმდებლობის, ორგანიზაციის პოლიტიკისა და სახელშეკრულებო ვალდებულებების შესაბამისად
- ჩვენი მომსახურების და პროცესების უსაფრთხოება მიმართულია რისკების იდენტიფიცირების და შესაბამისი კონტროლის განხორციელების და დოკუმენტირების მიმართ
- უნივერსიტეტის პერსონალისა და ვიზიტორის/კონტრაქტორის სამუშაო გარემო არის უსაფრთხო
- ბიზნესის უწყვეტობის და ინციდენტის რეაგირების გეგმები შენარჩუნებულია კომპანიის სტრატეგიული IT და ინფორმაციული მომსახურებისათვის და რეგულარულად ტესტირდება
- ჩვენი სახელით მომუშავე ყველა მესამე მხარე ასრულებს ბიზნეს პროცესების ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის მოთხოვნებს
- პოლიტიკა და ინფორმაციული უსაფრთხოების ცნობიერება მთელს კომპანიაში მუდმივად უმჯობესდება
- ინფორმაციული უსაფრთხოების სათანადო სწავლებები ტარდება პერსონალისა და სტუდენტებისათვის.

დამტკიცებულია:

საქართველოს უნივერსიტეტის რექტორის კონსტანტინე თოფურიას მიერ

01. 07. 2022 წ.