**ინფორმაციის კლასიფიკაციის პოლიტიკა**

ISO 9001 – ის მოთხოვნების მიხედვით

**ზოგადი დებულებები**

**1.1. დანიშნულება**

1. ინფორმაციის კლასიფიკაციის პოლიტიკა - დებულება სსიპ საქართველოს ტექნიკური უნივერსიტეტის უსაფრთხოების ზომების გამოყენების შესახებ და დოკუმენტური, მოქმედი ინფორმაციის უსაფრთხოების საკითხებზე. პროცედურის მოთხოვნებთან შესაბამისობა საშუალებას მოგცემთ ხარისხობრივად გამოიყენოთ ინფორმაციის უსაფრთხოების მართვის სისტემა, სსიპ საქართველოს ტექნიკური უნივერსიტეტის საინფორმაციო აქტივებისა და რესურსების დასაცავად.

2. პროცედურა შემუშავებულია პროცესების მფლობელების დასახმარებლად მონაცემთა მართვისთვის, ინფორმაციული აქტივების და რესურსების უსაფრთხოების დონის დასადგენად, რაც აუცილებელია ბიზნეს პროცესების შესასრულებლად და ორგანიზაციის მიზნების მისაღწევად.

**1.2. მოქმედების სფერო**

1. პროცედურა განისაზღვრება, როგორც სახელმძღვანელო სსიპ საქართველოს ტექნიკური უნივერსიტეტის ურთიერთობის ყველა მხარისთვის, რომლებსაც აქვთ წვდომა საინფორმაციო აქტივებსა და რესურსებზე, მათ შორის ინფორმაციული სისტემების პერსონალით, კონტრაქტორებით, ვიზიტორებით, დეველოპერებით და სხვ.

2. ამ პროცედურით განსაზღვრულ მეთოდებსა და დირექტივებს არ აქვთ მოქმედებებისა და ზომების ამომწურავი სია, რომლებიც უნდა უზრუნველყოფდეს სტაბილურობას, ბიზნეს პროცესების განხორციელებაში. სსიპ საქართველოს ტექნიკური უნივერსიტეტის სტრუქტურული ქვედანაყოფების ყველა ხელმძღვანელი უნდა გაეცნოს და იხელმძღვანელოს პროცედურაში აღწერილი ინფორმაციის კლასიფიკაციის მეთოდებით.

# 1.3. ტერმინები და განმარტებები

**QMS** - ხარისხის მენეჯმენტის სისტემა.

**IS** - ინფორმაციის უსაფრთხოება (კონფიდენციალურობის დაცვა, მთლიანობა და ინფორმაციის ხელმისაწვდომობა).

**რისკები** - გაურკვევლობის ეფექტი.

**აქტივები** - [რესურსი](https://uk.wikipedia.org/wiki/%D0%A0%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%B8), რომელთა გამოყენებას მომავალში ეკონომიკური სარგებელი მოაქვს.

**მფლობელი** - ტერმინი განსაზღვრავს პირს ან ორგანიზაციას, რომლისთვისაც დამტკიცებულია მენეჯმენტის პასუხისმგებლობა მოცემული რესურსის (აქტივის) წარმოების, განვითარების, შენარჩუნების, გამოყენებისა და უსაფრთხოების კონტროლზე.

# 1.4. მარეგულირებელი ცნობარი

**ISO 9001: 2015** ხარისხის მენეჯმენტის სისტემა. **ISO / IEC 27001: 2017** საინფორმაციო ტექნოლოგია.

# 2. პასუხისმგებლობისა და უფლებამოსილების დანაწილება

1. პროცედურაში აღწერილი პროცესის პასუხისმგებლობა ეკისრება იმ პირს, რომელიც პასუხისმგებელია ინტეგრირებული QMS და IS– ის ფუნქციონირებაზე.

2. ამ პროცედურის შეუსრულებლობამ ან არასათანადო შესრულებამ შეიძლება გამოიწვიოს საინფორმაციო აქტივებისა და რესურსების დაკარგვა უნივერსიტეტის წარმოების პროცესების შეწყვეტამდე და შესრულების მიზნების შეუსრულებლობა. პროცედურის სისტემური შეუსრულებლობა ან არასათანადო განხორციელება უნდა იქნას გამოკვლეული ინფორმაციული უსაფრთხოების ინციდენტის მართვის პროცესში, ინციდენტების აღრიცხვისა და რეაგირების წესის შესაბამისად.

# 3. პროცედურის აღწერა

# 3.1. ინფორმაციის კლასიფიკაციის კატეგორია

1. პროცედურით უნივერსიტეტის ინფორმაციული აქტივებისა და რესურსების ყველა მონაცემი იყოფა სამ კატეგორიად, ბიზნეს პროცესებზე გავლენის დონისა და ორგანიზაციის მიზნობრივი მაჩვენებლების მიხედვით:

|  |  |  |
| --- | --- | --- |
| **დონე** | **მნიშვნელობის კატეგორია** | **კონტროლის მოთხოვნები** |
| **I** | **მაღალი** | დარწმუნდით, რომ გააანალიზეთ და  გააკონტროლეთ |
| **ІІ** | **საშუალო** | აუცილებელია გარკვეული სიხშირით კონტროლი |
| **III** | **დაბალი** | საჭიროების შემთხვევაში მონიტორინგი |

2. ყველა კატეგორიის მნიშვნელობა დაცული უნდა იყოს ორგანიზაციის შიდა და გარე ინფორმაციული უსაფრთხოების დოკუმენტების შესაბამისად.

3. ყველა ინფორმაცია, შექმნილი, შენახული და დამუშავებული ინფორმაციული სისტემებში, რომლებიც ეკუთვნის უნივერსიტეტს და რომლებიც გამოიყენება ბიზნესის პროცესების ჩასატარებლად, კლასიფიცირდება მონაცემთა მნიშვნელობის სამი კატეგორიიდან ერთში. ასეთი ზომები ხორციელდება საინფორმაციო სისტემის ან რესურსის მართვისთვის, რომელიც უზრუნველყოფს მონაცემების მნიშვნელობას კატეგორიის მიხედვით.

4. მნიშვნელობის კატეგორიის მინიჭების მიზნით, პირველ რიგში უნდა შეფასდეს ინფორმაცია და მონაცემები ისეთი კრიტერიუმების შესახებ, როგორიცაა "K" კონფიდენციალობა, "C" მთლიანობა და "D" ხელმისაწვდომობა, ორგანიზაციის საქმიანობაზე ზემოქმედების ხარისხის გათვალისწინებით.

|  |  |
| --- | --- |
| **K კონფიდენციალურობის დონე** | **აღწერა** |
| 0 - საჯარო | ინფორმაციის გამოქვეყნება საიტებზე, მედიაში, სარეკლამო ბუკლეტები, პრეზენტაციები და სხვა საიმიჯო პროდუქტები. ამ ინფორმაციის გამჟღავნება (გაჟონვა) არ ახდენს უარყოფით  გავლენას უნივერსიტეტის საქმიანობაზე |
| 1 - უნივერსიტეტის შიდა საზოგადოება | ინფორმაცია, რომელიც წარმოდგენილია შიდა ვებგვერდზე, საჯარო განყოფილებებში, სერვერების საჯარო კატალოგებში, ინფორმაციის სტენდები. ამ ინფორმაციის გამჟღავნება (გაჟონვა)  უმნიშვნელო გავლენას ახდენს უნივერსიტეტის საქმიანობაზე |
| 2 - შიდა შეზღუდულია | სამუშაო დოკუმენტები და სტრუქტურული ერთეულების ჩანაწერები, პროექტები. ამ ინფორმაციაზე წვდომა რეგულირდება ინტეგრირებული QMS და IS– ის დოკუმენტებით ან სხვა დოკუმენტებით. ამ ინფორმაციის გამჟღავნება (გაჟონვა)  უმნიშვნელო გავლენას ახდენს უნივერსიტეტის საქმიანობაზე |
| 3 - კონფიდენციალური | ორგანიზაციული, ფინანსური, სატენდერო, მარკეტინგული ინფორმაცია, ინფორმაცია თანამშრომლების შესახებ, ქონების შეძენა და გასხვისება, თანამშრომლების ხელფასები, მომხმარებლები, მომწოდებლები, ხელშეკრულებები, პროექტები, ბიზნეს პროცესების ორგანიზება; ინფორმაცია, რომელიც საავტორო უფლებების საგანია (პროექტის შედეგები), სტრატეგიული განვითარების გეგმები და მიზნები ორგანიზაციულ დონეზე. ამ ინფორმაციის გამჟღავნება (გაჟონვა) მნიშვნელოვნად აისახება  უნივერსიტეტის საქმიანობაზე |
| 4 - მკაცრად  კონფიდენციალური | ინფორმაცია მკაცრად კონფიდენციალურია. ამ ინფორმაციის  გამჟღავნება (გაჟონვა) მნიშვნელოვან გავლენას ახდენს ორგანიზაციის საქმიანობაზე |
| **ხელმისაწვდომობის**  **დონეები "D"** | **აღწერა** |
| 0 - ძირითადი | რესურსი შეიძლება არ იყოს ხელმისაწვდომი 1 სამუშაო საათზე მეტი ხნის განმავლობაში |
| 1 - ნორმალური | რესურსი შეიძლება მიუწვდომელი იყოს 1 სამუშაო საათის განმავლობაში |
| 2 - საშუალო | რესურსი შეიძლება არ იყოს ხელმისაწვდომი 15 წუთის  განმავლობაში |
| 3 - მაღალი | რესურსი ხელმისაწვდომი უნდა იყოს მოთხოვნის საფუძველზე სამუშაო საათებში ნებისმიერ დროს |
| 4 - ძალიან მაღალი | რესურსი ყოველთვის ხელმისაწვდომი უნდა იყოს. მიუწვდომლობის დრო არ არის. |
| **მთლიანობის დონეები "C"** | **აღწერა** |
| 0 - ძირითადი | დაზიანება, არასანქცირებული რესურსის მოდიფიკაცია გავლენას არ ახდენს ორგანიზაციულ საქმიანობაზე, არ აქვს ფინანსური ზარალი. არანაირი გავლენა არ აქვს ორგანიზაციის იმიჯსა და  რეპუტაციაზე. რესურსის აღდგენა შესაძლებელია მოკლე დროში |
| 1 - ნორმალური | დაზიანება, არასანქცირებული რესურსის მოდიფიკაციამ შეიძლება გაართულოს გარკვეული ბიზნეს პროცესებისა და წარმოების ამოცანების შესრულება, რაც გამოიწვევს ბიზნეს პროცესების მცირე შენელებას. ფინანსური ზარალი უმნიშვნელოა. არანაირი გავლენა არ აქვს ორგანიზაცის იმიჯსა და რეპუტაციაზე. რესურსის სრული  აღდგენა შესაძლებელია სამუშაო საათებში |
| 2 - საშუალო | დაზიანება, არასანქცირებული რესურსის მოდიფიკაცია, რათა გაუჭირდეს გარკვეული ბიზნეს პროცესებისა და წარმოების ამოცანების შესრულება, რაც გამოიწვევს ბიზნეს პროცესების მცირე შენელებას. ფინანსური ზარალი საშუალოა. ორგანიზაციის იმიჯსა და რეპუტაციაზე გავლენა არ არსებობს ან უმნიშვნელოა. რესურსის  სრული აღდგენა შესაძლებელია, მაგრამ ამას დიდი დრო სჭირდება |
| 3 - მაღალი | რესურსის დაზიანებამ, უნებართვო მოდიფიცირებამ შეიძლება გამოიწვიოს ბიზნეს პროცესების მნიშვნელოვანი შენელება ან დროებითი შეჩერება. ფინანსური ზარალი მნიშვნელოვანია. ორგანიზაციის იმიჯსა და რეპუტაციაზე გავლენა საშუალოა.  რესურსების აღდგენა მხოლოდ ნაწილობრივ არის შესაძლებელი |
| 4 - ძალიან მაღალი | დაზიანებამ, რესურსის უნებართვო მოდიფიცირებამ შეიძლება გამოიწვიოს მნიშვნელოვანი ფინანსური ზარალი, ბიზნეს პროცესების სრული შეჩერება, უარყოფითად აისახოს  ორგანიზაციის იმიჯზე. რესურსის აღდგენა შეუძლებელია |

# 3.1.1. I კატეგორიის მნიშვნელობის მონაცემების განმარტება (მაღალი)

1. უნივერსიტეტის საინფორმაციო აქტივებისა და რესურსების მონაცემები, წარმოადგენს ორგანიზაციულ საიდუმლოებას, შეიცავს კონფიდენციალურ ინფორმაციას ან აქვთ სამართლებრივი დაცვა კანონმდებლობის მოთხოვნების შესაბამისად. მონაცემები, რომლებიც არ არის დაცული კანონით, დაცული უნდა იყოს ("K") წვდომის კონტროლის დაკარგვისგან ან ("C") უნებართვო შეცვლისგან, კონტრაქტორებთან, მომწოდებლებთან, დეველოპერებთან და ინფორმაციული სისტემების მწარმოებლებთან არსებული ხელშეკრულებების შესაბამისად (მაგალითად კონფიდენციალურობის შესახებ შეთანხმებების საფუძველზე). I კატეგორიის მონაცემთა სრული ჩამონათვალი განისაზღვრება მონაცემთა და ინფორმაციის მფლობელების მიერ რომელიც ასევე დადასტურებულია პროცესის მფლობელების მიერ.

|  |  |
| --- | --- |
| **მონაცემთა დაკარგვის მაგალითები** | **I კატეგორიის მნიშვნელობის**  **მონაცემების ზემოქმედების მაგალითები** |
| ლეპტოპი ან პორტატული საშუალებები მოიპარეს ოთახიდან ან დატოვეს სხვისი  ოთახში. | წარმოების პროცესის ეფექტურობის ხანგრძლივი დაკარგვა ერთეულის  დონეზე. |

|  |  |
| --- | --- |
| დასაშვები კოდები არ შეცვლილა თანამშრომლის გათავისუფლების ან საგარეო კონტრაქტორის შეცვლის შემდეგ, რომელიც ახლავს ინფორმაციულ სისტემას. | რეპუტაციის ან ფინანსური შედეგების ხანგრძლივი დაკარგვა |
| მესამე მხარე, რომელიც შემოვიდა შენობაში ან დარჩა უყურადღებოდ შენობაში, მოიპარა ტექნიკა ან მედია, ან გამოიყენა არასწორად წვდომა კომპიუტერზე ან სერვერზე. | ფინანსური ანალიტიკისა და მიზნების არასანქცირებული წვდომა. |

# 3.1.2. II კატეგორიის მნიშვნელობის მონაცემების განმარტება (საშუალო)

უნივერსიტეტის ინფორმაციული აქტივებისა და რესურსების მონაცემები, რომლებიც არ არის კლასიფიცირებული I კატეგორიის მნიშვნელობაში, მაგრამ გამოიყენება მარეგულირებელი ან ფისკალური ორგანოებისა და ადგილობრივი თვითმმართველობების მოთხოვნების საპასუხოდ, ან სხვა სპეციფიკური წარმოების შიდა ანგარიშების, ანალიტიკის, ბუღალტრული აღრიცხვისთვის. ასეთი მონაცემები დაცული უნდა იყოს შექმნის, შენახვისა და დამუშავების ლეგიტიმურობისა და ნამდვილობის უზრუნველსაყოფად.

|  |  |
| --- | --- |
| **მონაცემთა დაკარგვის მაგალითები** | **II მონაცემების ზემოქმედების მაგალითები -**  **მნიშვნელობის კატეგორია** |
| *I კატეგორიის ზემოთ მოყვანილი მაგალითების გარდა.*  ინფორმაციის მიმღებ თანამშრომელს არ აქვს შესაბამისი ნებართვა ან  დამტკიცება. | * რეპუტაციის ან ფინანსური საქმიანობის მოკლევადიანი დაკარგვა ადმინისტრაციული და წარმოების გადაწყვეტილებების გამო არასანდო მონაცემებზე დაყრდნობით. არსებობს ადმინისტრაციული და წარმოების გადაწყვეტილებების გაუქმების ან შეცვლის   შესაძლებლობა.   * წარმოების პროცესის ეფექტურობის მოკლევადიანი დაკარგვა დაწესებულების დამოუკიდებელი სტრუქტურული ერთეულის დონეზე. * არსებობს პირადი მონაცემების გამჟღავნების |

# 3.1.3. III კატეგორიის მნიშვნელობის მონაცემების განმარტება (დაბალი)

ინფორმაციული აქტივებისა და რესურსების მონაცემები, რომლებიც არ არის კლასიფიცირებული I-II მნიშვნელობის კატეგორიებში. ასეთ მონაცემებს არ აქვს მოთხოვნები ისეთი თვისებების მიმართ, როგორიცაა ("K") წვდომის კონტროლი, ("C") კანონიერი ცვლილების კონტროლი და ("D") გამოყენებადობა.

|  |  |
| --- | --- |
| **მონაცემთა დაკარგვის მაგალითები** | **III მონაცემების გავლენის მაგალითები -**  **მნიშვნელობის კატეგორიები** |
| *I-II კატეგორიის ზემოთ ჩამოთვლილი მაგალითების გარდა*  სასმელების დაღვრა კლავიატურაზე, ლეპტოპზე ან ქაღალდზე. | სამუშაო კომპიუტერის ან ლეპტოპის გამოყენების უნარის არარსებობა. პირადი მონაცემების დაკარგვა. |

ამ ინფორმაციულ სისტემებში შექმნილი, შენახული ან დამუშავებული მონაცემებისა და ინფორმაციის კლასიფიკაცია უნდა იქნას გამოყენებული ინფორმაციული სისტემების დაცვის დონის დასადგენად. მონაცემთა კლასიფიკაცია I კატეგორიის მნიშვნელობად ნებისმიერი თვისების მიხედვით საკმარისია ასეთი მონაცემების მნიშვნელობის უმაღლესი კატეგორიის დასადგენად, მაშინაც კი, თუ საინფორმაციო სისტემის ან რესურსების საცავები სხვადასხვა კატეგორიის მნიშვნელობის მონაცემებს ინახავს, ინფორმაციული სისტემა ან რესურსი უნდა დაექვემდებაროს დაცვის უმაღლეს დონეს, რაც განისაზღვრება ამ მონაცემების კლასიფიკაციით.

**4. მნიშვნელობის კატეგორიის განსაზღვრა მონაცემთა კლასიფიკაციით**

ინფორმაციის შეფასების და ანალიზის შემდეგ საჭიროა განისაზღვროს მისი კატეგორია და შენახვის მოთხოვნები.

|  |  |  |  |
| --- | --- | --- | --- |
| **ქონების შენახვის მოთხოვნა** | **I კატეგორიის** | **II კატეგორიის** | **III კატეგორია** |
| **"K" კონფიდენციალურობა** | 3-4 | 2 | 0-1 |
| **"C" მთლიანობა** | 3-4 | 2 | 0-1 |
| **"D" ხელმისაწვდომობა** | 3-4 | 2 | 0-1 |

მას შემდეგ, რაც უნივერსიტეტის საინფორმაციო აქტივებისა და რესურსების მონაცემები კლასიფიცირდება გარკვეული კატეგორიის მნიშვნელობად, პროცესების მფლობელებმა უნდა შეიტანონ ყველა გამოვლენილი ინფორმაცია (აქტივი) "ინფორმაციის აქტივების რეესტრში" (დანართი A).

# 5. ინფორმაციის კლასიფიკაცია ბიზნესის პროცესებზე ზემოქმედების ტიპის მიხედვით.

|  |  |  |  |
| --- | --- | --- | --- |
| **გავლენის ტიპი** | **კლასიფიკაციის სქემა** | | |
| **III - დაბალი** | **ІІ - საშუალო** | **და - მაღალი** |
| **1. ფინანსური** | ფინანსური ზარალი  100000 ლ-მდე. | ფინანსური ზარალი  100,000 ლ- დან. 1 000  000 ლ-მდე. | 1,000,000 ლ– ზე მეტი ფინანსური ზარალი. |
| **2. რეპუტაცია** | კრიტიკის რამდენიმე შემთხვევა  ადგილობრივ | კრიტიკის ზოგიერთი  შემთხვევა ეროვნულ | არასასურველი საზოგადოებრივი აზრი  ან კრიტიკა ეროვნული |

|  |  |  |  |
| --- | --- | --- | --- |
| **გავლენის ტიპი** | **კლასიფიკაციის სქემა** | | |
| **III - დაბალი** | **ІІ - საშუალო** | **და - მაღალი** |
|  | მედიაში | მედიაში | მთავრობის მხრიდან |
| **3. მარეგულირებელი** | გაფრთხილება მარეგულირებელი ორგანოსგან | ჯარიმები მარეგულირებელი ორგანოსგან | მარეგულირებელი ორგანოს მიერ  დაწესებული სანქციები და ორგანიზაციის საქმიანობის სხვა  შეზღუდვები, რაც  მნიშვნელოვნად აისახება  მის საქმიანობაზე |
| **4. ოპერაციული** | ბიზნეს პროცესების შეჩერების გარეშე | არაკრიტიკული - ბიზნეს პროცესების ნაწილობრივი  შეჩერება | კრიტიკული- ბიზნეს პროცესების შეჩერება |

# დანართი A. ინფორმაციული აქტივების რეესტრი

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **სახელი ან აღწერა** | **შენახვის ადგილი** | **მფლობელი** | **მომხმარებლები** | **კატეგორია დონის მიხედვით** | **გავლენის ტიპი** |
| **1** | **2** | **3** | **4** | **5** | **6** |
|  |  |  |  | K |  |
| D |
| C |
|  |  |  |  |  |  |
|  |
|  |
|  |  |  |  |  |  |
|  |
|  |

ახსნა:

სვეტი 1. მიუთითეთ კონკრეტული სახელი (მოწყობილობა, საკომუნიკაციო საშუალება, ინფორმაცია, მონაცემები), თუ ამის დაზუსტება შეუძლებელია, მოკლედ აღწერეთ;

სვეტი 2. მიუთითეთ ქვედანაყოფი, განყოფილება ან სხვა ადგილი, სადაც მდებარეობს მონაცემთა წყარო;

სვეტი 3. ტერმინი განსაზღვრავს პირს ან ორგანიზაციას, რომლის მენეჯმენტის მიერ დამტკიცებულია პასუხისმგებლობა ამ რესურსის (აქტივის) ISMS– ის წარმოებაზე, განვითარებაზე, შენარჩუნებაზე, გამოყენებასა და უსაფრთხოებაზე, ეს არ ნიშნავს, რომ პირს რეალურად აქვს ამ IA– ს ;

სვეტი 4. პირები, რომლებიც იყენებენ ამ IA– ს ყოველდღიურ მუშაობაში ან ერთჯერადად იყენებენ;

სვეტი 5. პროცედურა განსაზღვრავს სამ დონეს (K, D, C) და სამ კატეგორიას (I, II, III), მიუთითეთ დონე თითოეული კატეგორიისთვის, თუ ეს შესაძლებელია;

სვეტი 6. მიუთითეთ ზემოქმედების ტიპი პროცედურის შესაბამისად, შეიძლება იყოს რამდენიმე, ამ პროცედურაში არის ზემოქმედების ოთხი ტიპი, საჭიროების შემთხვევაში, სია შეიძლება გაფართოვდეს.