ინციდენტზე რეაგირების პოლიტიკა

1. ინციდენტზე რეაგირების პოლიტიკის მიზანი

შპს კენ ვოლკერის საერთაშორისო უნივერსიტეტისთვის მნიშვნელოვანია პერსონალურ მონაცემთა მაღალი ხარისხით დაცვა და უსაფრთხოების უზრუნველყოფა, ასევე მონაცემთა უსაფრთხოების დარღვევის ეფექტურად აღმოჩენა და სათანადო წესით რეაგირება. წინამდებარე დოკუმენტის მიზანია განსაზღვროს რეაგირების წესი იმ მონაცემთა უსაფრთხოების დარღვევის შემთხვევებზე, რომლებიც კვალიფიცირდება ინციდენტად და განსაზღვროს პასუხისმგებელი პირები აღნიშნულ პროცესში.

2. პირთა წრე, ვისზეც ვრცელდება ინციდენტზე რეაგირების პოლიტიკის დოკუმენტი

აღნიშნული პოლიტიკის დოკუმენტით განსაზღვრული წესი სრულად ვრცელდება შპს კენ ვოლკერის საერთაშორისო უნივერსიტეტის ხელმძღვანელობაზე, დასაქმებულ პერსონალზე და ყველა იმ მესამე პირზე, ვისაც რაიმე ფორმით შეიძლება ჰქონდეს შეხება იმ პერსონალურ მონაცემებთან, რომლებსაც უნივერსიტეტი ამუშავებს მისი საქმიანობის პროცესში.

3. ტერმინთა განმარტება

ინციდენტი - მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას /მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას;
მონაცემთა განადგურება - შემთხვევა, როდესაც მონაცემები საერთოდ აღარ არსებობს, ან აღარ არსებობს რაიმე გამოყენებადი ფორმით.

მონაცემთა დაზიანება - შემთხვევა, როდესაც მონაცემები შეიცვალა, გახდა არაზუსტი ან არასრული.

მონაცემთა დაკარგვა - შემთხვევა, როდესაც მონაცემები შესაძლოა კვლავ არსებობდეს, თუმცა, ისინი აღარ არის უნივერსიტეტის მფლობელობაში, ან როდესაც მონაცემები კვლავ უნივერსიტეტში ინახება, მაგრამ უნივერსიტეტს აღარ აქვს მათზე კონტროლი ან/და სათანადო წვდომა. წინამდებარე პოლიტიკის დოკუმენტში

გამოყენებულ სხვა ტერმინებს აქვთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

4. ინციდენტის სახეები

კონფიდენციალურობის დარღვევა – პერსონალური მონაცემების უნებართვო ან შემთხვევითი გამჟღავნება ან მათზე ამგვარი წვდომა.

მთლიანობის დარღვევა – პერსონალური მონაცემების უნებართვო შეცვლა, აგრეთვე, არამართლზომიერი ან შემთხვევითი დაზიანება, დაკარგვა.

ხელმისაწვდომობის დარღვევა – პერსონალურ მონაცემებზე წვდომის დაკარგვა, ან წვდომის უნებართვო შეზღუდვა ან დაზიანება, ასევე მონაცემების ამგვარი განადგურება ან წაშლა.

ზოგიერთი ინციდენტი შესაძლოა ერთდროულად არღვევდეს როგორც მონაცემთა კონფიდენციალურობის, ისე მთლიანობის ან/და ხელმისაწვდომობის პრინციპს.

5. პერსონალურ მონაცემებთან დაკავშირებული ინციდენტები

პერსონალურ მონაცემებთან დაკავშირებული ინციდენტების გამომწვევი მიზეზები შესაძლოა იყოს შემდეგი:

ქვევით მოცემულია გავრცელებული შემთხვევები, რა დროსაც ადგილი აქვს პერსონალურ მონაცემებთან დაკავშირებულ ინციდენტს:

- ადამიანური შეცდომა;
- მატერიალური ფორმით არსებული დოკუმენტების დაკარგვა ან მოპარვა;
- იმ ტექნიკის დაკარგვა ან მოპარვა, სადაც შენახულია პერსონალური მონაცემები;
- კონფიდენციალური მონაცემების განზრახ ან უნებლიე გამჟღავნება არაუფლებამოსილი მესამე მხარისთვის;
- კონფიდენციალურ ინფორმაციაზე არაავტორიზებული/არაუფლებამოსილი წვდომა;
- კიბერშეტევასთან (Hacking) დაკავშირებული ინციდენტი;
- პერსონალური მონაცემების, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების შემცველი ელექტრონული ფოსტის გაგზავნა სხვა ადრესატ(ებ)ისთვის/მესამე პირ(ებ)ისთვის;

- პერსონალური მონაცემების უყურადღებოდ დატოვება მარტივად ხელმისაწვდომ ადგილზე;
- შენობის დაყაჩაღება, გაქურდვა, დატბორვა, ხანძარი, ნგრევა და ა.შ.
- პერსონალური მონაცემების არასათანადო განკარგვა და სხვა.

იმ ფაქტის გათვალისწინებით, რომ ადამიანური შეცდომა ინციდენტის გამომწვევი მნიშვნელოვანი მიზეზი შეიძლება იყოს, უნივერსიტეტის თითოეული თანამშრომელი ვალდებულია პერსონალურ მონაცემებთან დაკავშირებით სათანადო სიფრთხილე გამოიჩინოს.

6. ინციდენტის ხარისხი

ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა **დაბალია** თუ ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს, **საშუალოა**, თუ ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნისა და ასეთი ზიანის/საფრთხის არარსებობის ალბათობა მეტნაკლებად თანაბარი და **მაღალია**, თუ – ინციდენტი დიდი ალბათობით მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

7. ინციდენტზე რეაგირების პროცედურა

ინციდენტზე რეაგირების პროცედურა შედგება შემდეგი 5 ეტაპებისგან:

- შეტყობინების მიღება;
- ინციდენტის დადასტურება;
- შეფასება
- აღრიცხვა და შეტყობინება
- პრევენცია

❖ შეტყობინების მიღება

ნებისმიერი პირი, ვისთვისაც ცნობილი გახდა ინციდენტის თაობაზე, ინციდენტის აღმოჩენისთანავე ან ასეთი ალბათობის შემთხვევაში, ინციდენტზე რეაგირების ჯგუფს უნდა შეატყობინოს ნებისმიერი მისთვის ხელმისაწვდომის საშუალებით

(სატელეფონო კომუნიკაცია, ელექტრონული ფოსტა, მოკლე ტექსტური შეტყობინება ან სხვა მისთვის ხელმისაწვდომი საკომუნიკაციო საშუალებით)

შეატყობინება უნდა მოიცავდეს შემდეგი სახის ინფორმაციას:

- ინციდენტის შესახებ ინფორმაციის წარმდგენი პირის ვინაობა და საკონტაქტო მონაცემები;
- ინციდენტის აღწერა;
- მონაცემთა კატეგორია, რომელსაც ეხება ინციდენტი;
- მონაცემთა სავარაუდო ოდენობა, რომელსაც ეხება ინციდენტი;
- ინციდენტის მდებარეობა;
- ინციდენტის დრო და ადგილი;
- სხვა დეტალები ინციდენტთან დაკავშირებით.

მნიშვნელოვანია, რომ ინციდენტის აღმომჩენმა პირმა ზემოაღნიშნული ინფორმაცია მიაწოდოს ინციდენტზე რეაგირების ჯგუფს მაშინვე, როდესაც მისთვის ცნობილი გახდება ინციდენტის შესახებ და არ დაელოდოს დამატებითი/კონკრეტული დეტალების მოძიებას/მოკვლევას ინციდენტთან დაკავშირებით.

იმ შემთხვევაში, თუ ინციდენტი აღმოჩენილია უნივერსიტეტის IT სამსახურის/თანამშრომლის მიერ, შესაბამისი პირი ვალდებულია დაუყონებლივ განახორციელოს ქმედებები, რათა აღმოფხვრას სისტემური ხარვეზი და შეამციროს შესაძლო საფრთხე.

აღნიშნული ქმედებები შესაძლოა მოიცავდეს:

- აპლიკაციების გათიშვას;
- ანგარიშების დახურვას;
- პაროლების შეცვლას;
- დაკარგული ინფორმაციის/დოკუმენტაციის მოძიებას;
- წვდომების შეზღუდვა/გაუქმებას და სხვა.

❖ ინციდენტის დადასტურება

ინციდენტთან დაკავშირებით შეტყობინების მიღებისთანავე ინციდენტზე რეაგირების ჯგუფი ახორციელებს სწრაფ მოკვლევას ინციდენტთან დაკავშირებით, მათ შორის, როდის მოხდა ინციდენტი და როდის მოხდა მისი აღმოჩენა, როგორ

მოხდა, რომელ მონაცემებზე რა სახის გავლენა მოახდინა. აღსანიშნავია, რომ ინციდენტზე რეაგირების ჯგუფი იქმნება უნივერსიტეტის რექტორის ბრძანებით. ინციდენტზე რეაგირების ჯგუფი დაკომპლექტებულია ისეთი პირებისგან, ვისაც გააჩნია ინციდენტის შეფასების კომპეტენცია. ჯგუფის სავალდებულო წევრს წარმოადგენს პერსონალურ მონაცემთა დაცვის ოფიცერი.

❖ შეფასება

ინციდენტზე რეაგირების ჯგუფი ვალდებულია განახორციელოს ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობისა და სიმძიმის შეფასება. აღნიშნული შეფასება უნდა განხორციელდეს ფაქტობრივი გარემოებების შეფასებით, ბრძანებით განსაზღვრული კრიტერიუმების შესაბამისად.

❖ აღრიცხვა შეტყობიება

თუ ინციდენტზე რეაგირების ჯგუფი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა საშუალო ან მაღალია, უნივერსიტეტი ვალდებულია აღრიცხოს იგი ინციდენტების რეესტრში და დაუყონებლივ, მაგრამ არაუგვიანეს ინციდენტის აღმოჩენიდან 72 საათისა, მის შესახებ შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს (შემდგომში - სამსახური) კანონისა და ბრძანებით განსაზღვრული წესის შესაბამისად. უნივერსიტეტი ინციდენტის შესახებ შეტყობინებას სამსახურს წარუდგენს ელექტრონული ან წერილობით ფორმით. ელექტრონული ფორმით შეტყობინებას უნივერსიტეტი წარადგენს სამსახურის შეტყობინების მართვის ელექტრონული სისტემის საშუალებით. წერილობითი ფორმით შეტყობინება სამსახურს წარედგინება უნივერსიტეტის მიერ დამტკიცებული ფორმის მიხედვით, რომელიც თან ერთვის წინამდებარე პოლიტიკის დოკუმენტს დანართი N1-ის სახით. თუ ინციდენტზე რეაგირების ჯგუფი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა მაღალია, უნივერსიტეტი ასევე ვალდებულია პირველი შესაძლებლობისთანავე, გაუმართლებელი დაყოვნების გარეშე აცნობოს მონაცემთა სუბიექტს ინციდენტის შესახებ და მარტივ და გასაგებ ენაზე მიაწოდოს შემდეგი ინფორმაცია:

- ინციდენტისა და მასთან დაკავშირებული გარემოებების ზოგადი აღწერა;

- ინციდენტით გამოწვეული სავარაუდო/დამდგარი ზიანი, მის შესამცირებლად ან აღმოსაფხვრელად განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ;
- პერსონალურ მონაცემთა დაცვის ოფიცრის ან სხვა პირის საკონტაქტო მონაცემები.

მონაცემთა სუბიექტის ინფორმირება უნდა განხორციელდეს ინდივიდუალურად თითოეული სუბიექტისათვის ელექტრონულ ფოსტაზე გაგზავნილი წერილობითი შეტყობინების გზით. თუ მონაცემთა სუბიექტის ინფორმირება არაპროპორციულად დიდ ხარჯებს ან ძალისხმევას მოითხოვს (მაგალითად, თუ მონაცემთა სუბიექტების წრე ფართოა და ა.შ), უნივერსიტეტი ინციდენტთან დაკავშირებულ ინფორმაციას გამოაქვეყნებს მის ვებსაიტზე საჯაროდ ხელმისაწვდომი ფორმით, ისე რომ ჯეროვნად იქნეს უზრუნველყოფილი მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების შესაძლებლობა. თუ ინციდენტზე რეაგირების ჯგუფი მიიჩნევს, რომ ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებებისათვის მნიშვნელოვანი ზიანის გამოწვევის ან/და მნიშვნელოვანი საფრთხის შექმნის ალბათობა დაბალია, ასეთი ინციდენტი ექვდემდებარება მხოლოდ ინციდენტების რეესტრში აღრიცხვას და ინივერსიტეტს არ ეკისრება შეტყობინების ვალდებულება სამსახურისათვის ან/და მონაცემთა სუბიექტისათვის.

❖ პრევენცია

ზემოაღნიშნული ღონისძიებების გატარებისა და ინციდენტთან დაკავშირებით აუცილებელი ზომების მიღების შემდგომ, ინციდენტზე რეაგირების ჯგუფმა უნდა მოიკვლიოს და გაანალიზოს ის პროცესები/მიზეზები, რამაც ინციდენტი გამოიწვია. რის შედეგადაც შესაძლოა გადარდეს შესაბამისი პრევენციული ღონიძიებები, კერძოდ: შიდა პოლიტიკის დოკუმენტების გადახედვა და ცვლილება, ახალი პოლიტიკის დოკუმენტების შემუშავება, თანამშრომელთა გადამზადება და ტრენინგი, სათანადო ხელშეკრულებებში ვალდებულებების განსაზღვრა, სისტემის ტექნიკური აუდიტი და ხარვეზების აღმოფხვრა, ანტივირუსული სისტემის განახლება და სხვა.

8. ინციდენტის აღრიცხვა

თითოეული ინციდენტი უნდა აღირიცხოს ინციდენტების რეესტრში, რომლის ფორმაც ერთვის წინამდებარე პოლიტიკის დოკუმენტს დანართი N2-ის სახით და წარმოადგენს მის განუყოფელ ნაწილს.

ინციდენტის რეესტრში აღირიცხება შემდეგი ინფორმაცია: 1. ინციდენტის აღწერა; 2. ინციდენტის დაწყებისა და დასრულების თარიღი; 3. პერსონალური მონაცემების კატეგორია, რომელზეც გავლენა მოახდინა ინციდენტმა; 4. პერსონალური მონაცემების ოდენობა, რომელზეც გავლენა მოახდინა ინციდენტმა; 5. ინციდენტის ხარისხი (მაღალი/საშუალო/დაბალი); 6. განხორციელდა თუ არა სამსახურისთვის შეტყობინება; 7. განხორციელდა თუ არა მონაცემთა სუბიექტების შეტყობინება. ინციდენტის რეესტრში ინფორმაცია ინციდენტის შესახებ ინახება 5 (ხუთი) წლის ვადით, რის შემდეგაც იგი ნადგურდება/იშლება პასუხისმგებელი პირის მიერ.

9. პერსონალურ მონაცემთა დაცვის ოფიცერი

პერსონალურ მონაცემთა დაცვის ოფიცერი წარმოადგენს ინციდენტზე რეაგირების ჯგუფის წევრს, რომელიც აქტიურად არის ჩართული ინციდენტის მართვის პროცესში. პერსონალურ მონაცემთა დაცვის ოფიცერი გასცემს რჩევებსა და რეკომენდაციებს, მონაწილეობს რისკების შეფასების პროცესში.

10. ინციდენტზე რეაგირების ჯგუფი

ინციდენტზე რეაგირების ჯგუფი ახორციელებს ინციდენტის მართვის პროცესს. ინციდენტის ჯგუფის წევრებს ამტკიცებს რექტორი შესაბამისი ბრძანების საფუძველზე.

11. ცვლილებები პოლიტიკაში

უნივერსიტეტი იტოვებს უფლებას ნებისმიერ დროს განაახლოს აღნიშნული პოლიტიკა, რომელიც განთავსდება უნივერსიტეტის ვებ გვერდზე(ასეთის არსებობის შემთხვევაში), ასევე უნივერსიტეტის შენობაში ხელმისაწვდომ ადგილას.

დანართი N1

ინციდენტის შეტყობინების ფორმა	
პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი	
სახელწოდება	
სამართლებრივი ფორმა	
საიდენტიფიკაციო ნომერი	
მისამართი	
▪ **პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირის საქმიანობის სფერო**	
□ კერძო სექტორი □საჯარო სექტორი □სამართალდამცავი ორგანო	
ინციდენტის შეტყობინების ფორმის შევსებაზე პასუხისმგებელი პირის მონაცემები	
სახელი	
გვარი	
პოზიცია/თანამდებობა	
ტელეფონის ნომერი	
ელ-ფოსტა	
არსებობის შემთხვევაში, ინფორმაცია პერსონალურ მონაცემთა დაცვის ოფიცრის შესახებ	
სახელი	
გვარი	
ტელეფონის ნომერი	
ელ-ფოსტა	
არსებობის შემთხვევაში, სხვა საკონტაქტო პირის მონაცემები	

სახელი	
გვარი	
პოზიცია/თანამდებობა	
ტელეფონის ნომერი	
ელ-ფოსტა	
ინფორმაციის/შეტყობინების სახე	
□პირველადი □დამატებითი□განახლებული	
დამატებითი ან განახლებული ინფორმაციის/შეტყობინებისთვის მინიჭებული საიდენტიფიკაციო ნომერი	
ინციდენტის სტატუსი	
□მიმდინარე □დასრულებული □დაუდგენელი	
ინციდენტის დაწყების დრო	
საათი	
დღე	
თვე	
წელი	
ინციდენტის დასრულების დრო	
საათი	
დღე	
თვე	
წელი	
დამუშავებისთვის პასუხისმგებელი პირის მიერ ინციდენტის აღმოჩენის დრო	
საათი	

დღე	
თვე	
წელი	

იმ შემთხვევაში, თუ შეტყობინებით ინციდენტის შესახებ ინფორმაციის სამსახურისთვის სრულად მიწოდება ვერ ხორციელდება, განმარტება აღნიშნულის მიზეზის თაობაზე

ინციდენტის სახე

□კონფიდენციალურობის დარღვევა □ხელმისაწვდომობის დარღვევა□მთლიანობის დარღვევა

ინციდენტის შედეგები

□ მონაცემების შემთხვევით ან განზრახ განადგურება

□მონაცემების შემთხვევით ან განზრახ შეცვლა

□დაშიფრული მოწყობილობის მოპარვა ან დაკარგვა

□დაუშიფრავი მოწყობილობის მოპარვა ან დაკარგვა

□მატერიალური დოკუმენტის მოპარვა ან დაკარგვა

□მატერიალური დოკუმენტის მოპარვა, დაკარგვა ან მასზე უნებართვო წვდომა

□ელექტრონული ფორმით არსებულ მონაცემებზე უნებართვო წვდომა;

□ელექტრონული ან/და მატერიალური ფორმით არსებულ მონაცემებზე წვდომის შესაძლებლობის შეზღუდვა;

□ვიდეომონიტორინგის ან/და აუდიომონიტორინგის სისტემის მეშვეობით დამუშავებულ მონაცემებზე უნებართვო წვდომა/მათი უკანონო გამჟღავნება

□ელექტრონული ფოსტით განხორციელებულ მიმოწერაზე უნებართვო წვდომა/მისი უკანონო გამჟღავნება

□ონლაინ პორტალზე არსებულ მომხმარებლის ანგარიშზე უნებართვო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება

□სოციალური მედიის ან/და მოკლე ტექსტური შეტყობინებების მიმოცვლის პლატფორმაზე არსებულ მომხმარებლის ანგარიშზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება;

□საფოსტო კორესპონდენციაზე უკანონო წვდომა/მასში არსებული მონაცემების უკანონო გამჟღავნება;

□ელექტრონულ მოწყობილობაში შენახულ მონაცემებზე უკანონო წვდომა;

□მონაცემების ზეპირსიტყვიერად გამჟღავნება

□მონაცემებზე წვდომის მოპოვება მოტყუების ან შეცდომაში შეყვანის გზით;

□მონაცემების უკანონო გასაჯაროება;

□მონაცემთა დამუშავებისას დაშვებული შეცდომა;

□სისტემის ტექნიკური გამართულობის უზრუნველსაყოფად საჭირო სამუშაოები;

□ხვა შედეგი;

ინფორმაცია მონაცემებზე რომელზეც ინციდენტი გავლენას ახდენს

□სახელი, გვარი, დაბადების თარიღი;

□პირადი ან/და პასპორტის ნომერი;

□საკონტაქტო მონაცემები;

□საიდენტიფიკაციო ან წვდომის ინფორმაცია (მომხმარებლის სახელი, პაროლი);

□სოციალური მედიის გვერდი (ე.წ. პროფილი);

□ეკონომიკური და ფინანსური მონაცემები;

□ოფიციალური დოკუმენტები ან მათი ასლები;

□ადგილმდებარეობის მონაცემები (მათ შორის, გეოლოკაციის შესახებ ინფორმაცია);

□პერსონალური მონაცემების შემცველი ფოტო, ვიდეო ან აუდიომასალა;

□პირად საქმიანობასთან ან ოჯახურ ცხოვრებასთან დაკავშირებული ინფორმაცია; □პროფესიულ საქმიანობასთან დაკავშირებული ინფორმაცია; □პირის მიერ განხორციელებული კომუნიკაციის ამსახველი მონაცემები; □განსაკუთრებული კატეგორიის მონაცემები; □სხვა მონაცემი; □მონაცემები ცნობილი არ რის
მონაცემთა სუბიექტების სავარაუდო ან ზუსტი რაოდენობა, რომლებზეც ინციდენტი გავლენას ახდენს

□რაოდენობა უცნობია		
□რაოდენობა ცნობილია და შეადგენს		

უკავშირდება თუ არა ინციდენტის შედეგი არასრულწლოვანს, შეზღუდული შესაძლებლობების მქონე პირს ან/და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე პირს
□დიახ □არა □არ არის ცნობილი
როგორია ალბათობა იმისა, რომ ინციდენტი გამოიწვევს ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვან ზიანს/მნიშვნელოვან საფრთხეს
□საშუალო □მაღალი
ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების (მონაცემთა უსაფრთხოების უზრუნველმყოფი ტექნიკური, პროგრამული და ფიზიკური უსაფრთხოების გადაწყვეტები/მექანიზმები, ორგანიზაციული ფორმალიზებული არაფორმალიზებული წესები) შესახებ, რომლებიც ინციდენტის შემდეგ გატარდა

ინფორმაცია მონაცემთა უსაფრთხოების და ინციდენტის შედეგად მოსალოდნელი ზიანის შემცირების უშუალოდ ხელშემწყობი იმ ტექნიკური ან/და ორგანიზაციული ზომების (მონაცემთა უსაფრთხოების უზრუნველმყოფი ტექნიკური, პროგრამული და

ფიზიკური უსაფრთხოების გადაწყვეტები/მექანიზმები, ორგანიზაციული ფორმალიზებული პოლიტიკები არაფორმალიზებული წესები) შესახებ, რომელთა გატარებაც სამომავლოდ იგეგმება
გეგმავს თუ არა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ინციდენტის შესახებ მონაცემთა სუბიექტ(ებ)ის ინფორმირებას, რა ვადაში და რა ფორმით
შეუქმნის თუ არა ინციდენტის შესახებ ინფორმაციის გასაჯაროება საფრთხეს:
□სახელმწიფო უსაფრთხოების, ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების ან/და თავდაცვის ინტერესებს; □საზოგადოებრივი უსაფრთხოების ინტერესებს □დანაშაულის თავიდან აცილებას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას, მართლმსაჯულების განხორციელებას, პატიმრობისა და თავისუფლების აღკვეთის აღსრულებას, არასაპატიმრო სასჯელთა აღსრულებას და პრობაციას, ოპერატიულ-სამძებრო საქმიანობას; □ქვეყნისთვის მნიშვნელოვან ფინანსურ ან ეკონომიკურ (მათ შორის, მონეტარულ, საბიუჯეტო და საგადასახადო), საზოგადოებრივი ჯანმრთელობისა და სოციალური დაცვის საკითხებთან დაკავშირებულ ინტერესებს;
კანონის 29-ე მუხლის მე-11 პუნქტით გათვალისწინებულ შემთხვევაში, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების სფეროში შესაბამის კომპეტენტურ უწყებასთან შეთანხმების თაობაზე ინფორმაცია

დანართი N2

ინციდენტის რეესტრი	
ინციდენტის აღწერა	
ინციდენტის დაწყების თარიღი	
ინციდენტის დასრულების თარიღი	
პერსონალური მონაცემების კატეგორია, რომელზეც გავლენა მოახდინა ინციდენტმა	
პერსონალური მონაცემების ოდენობა, რომელზეც გავლენა მოახდინა ინციდენტმა	
ინციდენტი სხარისხი (მაღალი/საშუალო/დაბალი)	
განხორციელდა თუ არა სამსახურისთვის შეტყობინება	
განხორციელდა თუ არა მონაცემთა სუბიექტების ინფორმირება	