**ინციდენტების აღრიცხვის ფორმა ინციდენტის N: −**

ინსტრუქცია:

1. **ინციდენტის ან მნიშვნელოვანი მოვლენის შეტყობინება საქართველოს ეროვნული ბანკისთვის:** 
   * იხილეთ სექცია (ა); და
   * იხილეთ დანართი, თუ ეს არის კიბერუსაფრთოხების ინციდენტი.
2. **შემდგომი განახლება(ები) (განახლებები, როდესაც მიმდინარე მოვლენაში ცვლილებებია ან საქართველოს ეროვნული ბანკისგან არის მოთხოვნილი):**
   * განახლებები წარმოადგინეთ სექცია (ა)-ში; და
   * კიბერუსაფრთხოების განახლებები წარადგინეთ დანართში.
3. **სრული ინციდენტების ანგარიში (რელევანტური სამართლებრივი ჩარჩოს მოთხოვნისამებრ):**
   * წარადგინეთ სექცია (ა) და (ბ)

|  |  |
| --- | --- |
| **სექცია (ა) 1-3** | |
| 1. **დეტალები:** |  |
| * სებ-ისთვის მყისიერი შეტყობინების დრო და თარიღი |  |
| * ფინანსური ინსტიტუტის სრული დასახელება |  |
| * ფორმის შევსებაზე/ანგარიშგებაზე პასუხისმგებელი პირი |  |
| * თანამდებობა/დეპარტამენტი |  |
| * საკონტაქტო ინფორმაცია (ტელ, ელ-ფოსტა) |  |
| 1. **მოვლენის დეტალები:** |  |
| * მოვლენის აღმოჩენის დრო და თარიღი |  |
| * მოვლენის სახეობა/ზემოქმედების არეალი:  1. **IT სისტემის შეფერხება** (მაგ core banking systems, ბანკომატი, გადახდის სისტემები როგორიცაა EFTPOS, CTS, GIRO, MEPS+, CLS) 2. **კიბერუსაფრთხოების მოვლენა** *(მაგ.: ჰაკინგი, ფიშინგი)* 3. **ინფორმაციის მოპარვა (ფიზიკურად) ან დაკარგვა***(მაგ.: როდესაც მგრძნობიარე /მნიშვნელოვანი/სამომხმარებლო ინფორმაცია მოპარული ან დაკარგულია)* 4. **ინფრასტრუქტურის გაუმართაობა***(მაგ., ელექტროენერგია,წყალი,გაზი, ტელეკომუნიკაცია,ხანძარი)* 5. **ფინანსური** *(მაგ., ლიკვიდურობა, დეპოზიტების მნიშვნელოვანი გადინება)* 6. **დასაქმებულთა მიუწვდომლობა** (მაგ,თანამშრომლებისგან გამოწვეული დანაკარგები ან მათი დაუსწრებლობა) 7. **სხვა** *(მაგ., აუთსორსინგული მომსახურების მიმწოდებლები, კანონის/რეგულაციის დარღვევა)* |  |
| * რა ქმედებები ან რეაგირება განხორციელდა ფინანსური ინსტიტუტის მიერ? |  |
| 1. **ზემოქმედების შეფასება** |  |
| * მოვლენის გავლენა ბიზნესზე და მომსახურების ხელმისაწვდომობაზე – სახაზინო მომსახურება, ფულადი სახსრების მართვა, ფილიალები, ATMs, ინტერნეტ ბანკინგი და ა.შ. |  |
| * გავლენა დაინტერესებულ მხარეებზე − ზემოქმედების ქვეშ მოქცეული საცალო/კორპორატიული კლიენტები, დაზარალებული მონაწილეები, ოპერატორების, სერვისის მომწოდებლების და ანგარიშსწორების განმახორციელებელი ინსტიტუტების ჩათვლით |  |
| * ფინანსურ ბაზარზე − ვაჭრობის, ტრანზაქციების რაოდენობის და ღირებულების, მონეტარული დანაკარგების, ლიკვიდობის, თანხების გადინების შედეგი |  |
| * საზედამხედველო და იურიდიული გავლენა |  |
| **სექცია (ბ) 4-6** | |
| 1. **მოვლენის დეტალური ქრონოლოგიური მიმდევრობა:** |  |
| * ინციდენტის თარიღი, დაწყების დრო და ხანგრძლივობა |  |
| * რა ზომა/ები მიიღო ორგანიზაციამ მოცემული მოვლენის გავლენის შესამცირებლად? რატომ? |  |
| * ინფორმირებული და პროცესში მონაწილე დაინტერესებული მხარეები |  |
| * რა საკომუნიკაციო არხები იქნა გამოყენებული? |  |
| * BCP-ის გააქტიურების მიზეზი |  |
| 1. **გამომწვევი მიზეზების დეტალური ანალიზი** |  |
| * ფაქტორები და მიზეზები, რამაც გამოიწვია პრობლემა |  |
| * პრობლემის გადასაჭრელად/გასაბათილებლად გადადგმული ნაბიჯები |  |
| * იდენტიფიცირებული პროცესები, რომელთა განხორციელება იქნება მიმართული ინციდენტის აღმოსაფხვრელად სამომავლოდ |  |
| 1. **საბოლოო შეფასება და აღდგენა:** |  |
| * დასკვნა ინციდენტის მიზეზსა და შედეგებზე |  |
| * ჩამოთვალეთ მაკორექტირებელი ქმედებები, რომლებიც განხორციელდა, რათა სამომავლოდ აღარ განმეორდეს მსგავსი ტიპის ინციდენტები |  |
| * ინციდენტის გადაწყვეტის თარიღი \_\_\_\_\_\_\_\_\_ (DD/MM/YY). |  |

**დანართი**

|  |  |  |  |
| --- | --- | --- | --- |
| **კიბერუსაფრთხოების ანგარიშგების ფორმა** | | | |
| **სექცია (A): ზოგადი ინფორმაცია No:** | | | |
|  | | | |
| ა(1). მოვლენა არის ახალი დაფიქსირებული მოვლენის განახლება   * პირველი განახლებისთვის მიუთითეთ „1“. თუ განახლება უკვე დაფიქსირებულ მოვლენას ეხება, გთხოვთ მიუთითოთ განახლების თანმიმდევრობის ნომერი.   თანმიმდევრობა No:გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი | | | |
| ა(2). რომელ კატეგორიაში კლასიფიცირდება მოვლენა | | | |
| კატეგორია 1  კრიტიკული სისტემის დაზიანება | კატეგორია 2  ინციდენტი დაფიქსირდა სისტემაში ან ქსელში, რომელსაც შეეძლო სისტემის დაზიანება | კატეგორია 3  ინციდენტი არ შეეხო კრიტიკულ სისტემას | |
| **სექცია B: ინციდენტი** | | | |
| B1. როდის შეატყობინეთ აღმასრულებელ მენეჯმენტს ინციდენტის შესახებ?  (გთხოვთ მიუთითოთ საქართველოს ადგილობრივი დრო (+4GMT))  თარიღი: გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ თარიღი | | | |
| B2. საფრთხეების/ინციდენტების ტიპები (თქვენ შეგიძლიათ აირჩიოთ ერთ პუნქტზე მეტი)  სერვისის ხელმიუწვდომლობის შეტევა (DoS)  სერვისის ხელმიუწვდომლობის განაწილებული შეტევა(DDoS)  ვირუსი/ჭია(მავნე პროგრამა)/ტროიანი  შეჭრა/არაავტორიზებული წვდომა  ვებგვერდის სახეცვლილება  სისტემის ბოროტად გამოყენება/არასათანადო გამოყენება  სხვა: გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი | | | |
| B3. დაკავშირებულია ეს ინციდენტი სხვა, ადრეშეტყობინებულ ინციდენტთან?  გთხოვთ აირჩიოთ   * თუ დიახ, გთხოვთ მიუთითოთ დამატებითი ინფორმაცია, როგორ არის ეს ინციდენტები ურთიერთდაკავშირებული   გთხოვთ, დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი   * გთხოვთ, მოგვაწოდოთ ადრეშეტყობინებული ინციდენტის ნომერი   ინციდენტის ნომერი: დააჭირეთ აქ, რომ შეიყვანოთ ტექსტი | | | |
| **სექცია C: ინციდენტის დეტალები** | | | |
| C1. გთხოვთ მიუთითოთ ინციდენტის დეტალები ქვემოთ მოცემულ გრაფაში   * როდის დაფიქსირდა ინციდენტის პირველი შემთხვევა?   გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი   * როგორ აღმოაჩინეთ/დააფიქსირეთ/გამოავლინეთ პირველი ინციდენტი?   გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი  C2. გთხოვთ მიუთითეთ კრიტიკული სისტემ(ებ)ის ან ქსელ(ებ)ის დეტალები რომელ(ებ)ზეც გავლენა იქონია ინციდენტმა.  დეტალები სულ მცირე უნდა მოიცავდეს:  *-ადგილმდებარეობა, მოცემული სისტემის/ქსელის დანიშნულება, დაზიანებული პროგრამები (მათ შორის აპარატურის მწარმოებელი, პროგრამული უზრუნველყოფის მწარმოებელი, წარმოების სერია/მოდელი, ა.შ.) გაშვებული სისტემაზე/ქსელზე, ა.შ.*  გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი  საჭიროების შემთხვევაში გთხოვთ მიუთითოთ დაზიანებული კრიტიკული სისტემ(ებ)ის ოპერაციული სისტემის დასახელება და ვერსიულობა  გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი  C3. რა ზეგავლენა იქონია შემოტევამ? (გთხოვთ *ამოარჩიოთ ერთი მონიშვნის უჯრა თითოეული სვეტისთვის*)   |  |  |  | | --- | --- | --- | | მომსახურების მიწოდება | სენსიტიური ინფორმაციის დანაკარგი | საზოგადოებრივი ნდობა და რეპუტაცია | | ზემოქმედების გარეშე | დანაკარგის გარეშე | ზემოქმედების გარეშე | | უმნიშვნელო ზემოქმედება | უმნიშვნელო დანაკარგი | უმნიშვნელო ზემოქმედება | | საშუალო ზემოქმედება | საშუალო დანაკარგი | საშუალო ზემოქმედება | | მნიშვნელოვანი ზემოქმედება | მნიშვნელოვანი ზემოქმედება | მნიშვნელოვანი ზემოქმედება | | კრიტიკული ზემოქმედება | კრიტიკული დანაკარგი | კრიტიკული ზემოქმედება |   C4. ჰქონდა დაზიანებულ კრიტიკულ სისტემ(ებ)ას/ქსელ(ებ)ს პოტენციური ზეგავლენა სხვა ფინანსური ინსტიტუტის კრიტიკულ აქტივ(ებ)ზე?  გთხოვთ ამოარჩიოთ   * თუ „დიახ“, გთხოვთ მიუთითოთ დამატებითი დეტალები:   გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი | | | |
| **სექცია D: ინციდენტის მართვის სტატუსი** | | |
| D1.  რა სახის ქმედებები განახორციელეთ ამ დროს?  გთხოვთ დააჭირეთ აქ, რომ შეიყვანოთ ტექსტი  D2. რა არის ამ ინციდენტის მიმდინარე სტატუსი?  გთხოვთ აირჩიოთ  თუ ინციდენტი არ არის მოგვარებული, რა არის შემდეგი მოქმედების ეტაპი?  გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი  D3. რა არის შემოტევის ან სისტემაში შეღწევის ყველაზე ადრე ცნობილი თარიღი?  *(თუ უცნობია, მონიშნეთ შესაბამისი უჯრა)*  (გთხოვთ მიუთითოთ საქართველოს ადგილობრივი დრო (+4GMT))  თარიღი: გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ თარიღი უცნობი:  D4. რა არის ინციდენტის წყარო/მიზეზი? (თუ უცნობია, ჩაწერეთ „უცნობია“)  გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი  D5. თუ შეატყობინეთ ინციდენტის შესახებ სამართალდამცავ ორგანოებს?  გთხოვთ აირჩიოთ   * თუ დიახ, მიუთითეთ ის ორგანო, ვისაც შეატყობინეთ;   გთხოვთ დააჭიროთ აქ, რომ შეიყვანოთ ტექსტი. | | |
| **სექცია E: სხვა ინფორმაცია** | | |
| E1. IP მისამართები(*მოითხოვება, თუ გამოვლინდა ინციდენტის დროს*)  გთხოვთ, მიუთითეთ ინციდენტიდან გამოვლენილი IP მისამართების სია. გთხოვთ მიუთითოთ IP მისამართების ჩართულობა ინციდენტში (მაგ.: Victim, მავნე კოდის ბრძანება & მთავარი სერვერები და სხვები). თუ IP მისამართები გამოვლინდა დომეინის სახელებიდან, გთხოვთ, მიუთითოთ დომეინის სახელები და IP მისამართების დომეინის სახელებიდან ნებართვის(რეზოლუციის) თარიღი/დრო.   |  |  |  |  | | --- | --- | --- | --- | | IP მისამართი | ჩართულობა | დომეინის სახელი საიდანაც გამოვლინდა IP მისამართი | IP მისამართის დომეინის სახელიდან რეზოლუციის თარიღი/დრო | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   E2. დომეინის სახელები (*მოითხოვება, თუ გამოვლინდა ინციდენტის დროს*)  გთხოვთ მიუთითეთ ინციდენტიდან გამოვლენილი დომეინების სია. გთხოვთ მიუთითოთ ინციდენტში დომეინის სახელების ჩართულობა (მაგ.: თანმდევი ჩამოტვირთვის სერვერები, მავნე კოდის კონტროლი & მართვის სერვერი, დაზიანებული ვებგვერდი)   |  |  | | --- | --- | | დომეინის სახელი | დომეინის სახელის ჩართულობა | |  |  | |  |  | |  |  | |  |  |   E3. ელექტრონული ფოსტის მისამართები (*მოითხოვება, თუ გამოვლინდა ინციდენტის დროს*)  მიუთითეთ ინციდენტიდან გამოვლენილი ელექტრონული ფოსტის მისამართების სია. გთხოვთ მიუთითოთ ინციდენტში ელექტრონული ფოსტის მისამართების ჩართულობა. მაგალითად, ელექტრონული ფოსტის მისამართი, რომლიდანაც ფიშინგის ელექტრონული ფოსტა გამოჩნდა და სხვ.   |  |  | | --- | --- | | ელ. ფოსტის მისამართი | ელ. ფოსტის ჩართულობა | |  |  | |  |  | |  |  | |  |  | |  |  |   E4. ინფორმაცია მავნე ფაილების შესახებ (*მოითხოვება, თუ გამოვლინდა ინციდენტის დროს*)  მიუთითეთ ინფორმაცია ინციდენტში მუქარის ფაილების გამოვლენის შესახებ, ქვემოთ მოცემულ ცხრილში:   |  |  |  |  | | --- | --- | --- | --- | | ფაილის სახელი | ზომა | MD5 ჰეში | ჩატარდა თუ არა ტექნიკური ანალიზი(დიახ/არა) | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | | |