კლიენტთა ინფორმაციის დაცვის უზრუნველყოფა დასტაში

27 ოქტომბერი, 2017წელი

შესავალი

აღნიშნული დოკუმენტი აღწერს, თუ როგორ იცავს დასტა კლიენტების ინფორმაციას ინფორმაციული უსაფრთხოებისა და ფიზიკური უსაფრთხოების საუკეთესო პრაქტიკების გამოყენებით. უპირველეს ყოვლისა, დასტა ეყრდნობა ინფორმაციული უსაფრთხოების სამ ძირითად პრინციპს: კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა. ფიზიკური უსაფრთხოების დაცვის მიმართულებით, დასტას გააჩნია 24/7 ცოცხალი დაცვა, მუდმივი ვიდეო-მეთვალყურეობის სისტემა, ხანძარსაწინააღმდეგო სისტემა, მსხვრევისა და მოძრაობის დეტექტორები, დაშვების ელექტრონული ავტორიზაცია და გარემოს საფრთხეებისგან დამცავი სისტემები. როგორც ფიზიკური ასევე ინფორმაციული უსაფრთხოების პროგრამების თითოეული ასპექტი დოკუმენტირებულია და რეგულარულად გადის აუდიტს.

ინფორმაციული უსაფრთხოება

დასტას ინფორმაციული უსაფრთხოების პროგრამა ფოკუსირებას ახდენს სამ ძირითად პრინციპზე: კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა.

კონფიდენციალობა მოიცავს წვდომის შეზღუდვას პირებისთვის, რომლებიც არ არიან ავტორიზებულნი. არსებობს საფრთხის ორი ძირითადი წყარო: შიდა და გარე.

შიდა საფრთხეები - მიუხედავად იმისა, რომ დასტას თანამშრომლებს რეგულარულად აქვთ წვდომა კონფიდენციალურ ინფორმაციაზე, როგორც მათი სამუშაოს განუყოფელი ნაწილი, ჩვენ მათ მხოლოდ იმ ტიპის ინფორმაციაზე ვანიჭებთ წვდომას, რომელიც საჭიროა მათი საქმიანობისთვის. ჩვენ რეგულარულად ვახორციელებთ წვდომის კონტროლის აუდიტს, რათა დავრწმუნდეთ, რომ თანამშრომლებს აქვთ წვდომა მხოლოდ იმ ინფორმაციაზე, რაც საჭიროა მათთვის. ეს გადახედვები არ მოიცავს მხოლოდ წვდომის შემოწმებას ინფორმაციაზე, რომელიც განთავსებულია სერვერებზე, ასევე მოწმდება წვდომები სპეციფიკურ პროგრამულ უზრუნველყოფაზე და ტერიტორიებზე (რომლებიც იმართება ელექტრუნული წვდომის კონტროლის სისტემით). გარდა ამისა, ჩვენ თანამშრომლებისთვის რეგულარულად ვატარებთ ტრენინგებს ინფორმაციულ უსაფრთხოებაში.

ჩვენ ასევე გვაქვს რიგი პოლიტიკები, რომელთა შესრულება სავალდებულოა დასტას ყველა თანამშრომლისთვის, კერძოდ:

- ინფორმაციული უსაფრთხოების პოლიტიკა
- კომპიუტერული მოწყობილობების მისაღები გამოყენების პოლიტიკა
- ელექტრონული ფოსტის პოლიტიკა
- სუფთა მაგიდის პოლიტიკა
- პაროლების პოლიტიკა
- ფიზიკური აქტივების უსაფრთხოებისა და წვდომის პოლიტიკა

გარდა ამისა, ჩვენ ვიყენებთ ინფორმაციის გაჟონვისგან თავის დაცვის მეთოდებს. თანამშრომლებს, სპეციალური ნებართვის გარეშე, არ აქვთ უფლება გამოიყენონ ინფორმაციის

გარე მატარებლები, როგორიცაა USB Flash დისკები, CD-დისკები ან მიიღონ წვდომა რისკის შემცველ ვებ-გვერდებზე, მაგალითად პერსონალური ელექტრონული ფოსტის ან ფაილების გაზიარების სერვისებზე. ასევე, ჩვენ ვიყენებთ ელექტრონული ფოსტის ფილტრაციასა და წესებს, რომლებიც იძლევა გარანტიას, რომ კონფიდენციალური ინფორმაცია ელექტრონული ფოსტით არ დატოვებს ორგანიზაციას.

იმისთვის, რომ თავიდან ავიცილოთ ფიზიკური დოკუმენტების გაჟონვა, ჩვენ ვიყენებთ ვიდეო-მეთვალყურეობის სისტემას ყველა ოთახში, სადაც ხდება დოკუმენტების დამუშავება. არა-უსაფრთხო ზონებში დოკუმენტების გატანა აკრძალულია. ასევე, თანამშრომლებს დაცულ ზონებში არ აქვთ უფლება შეიტანონ ხელჩანთები ან ქურთუკები და გამოიყენონ მობილური ტელეფონები.

ჩვენ ასევე ვაკეთებთ თანამშრომელთა სკრინინგს, რომელიც მოიცავს ცნობას ნასამართლეობის შესახებ, საკრედიტო ინფორმაციას, შემოწმებას ნარკოტიკულ საშუალებების მოხმარებაზე. ყოველივე ეს თანამშრომელთა მორალური რეპუტაციის მაქსიმალური დონის შენარჩუნებას უზრუნველყოფს.

გარე საფრთხეები - მესამე პირი, რომელიც არ არის ჩვენი კლიენტის მიერ ავტორიზებული ვერასოდეს მიიღებს წვდომას ინფორმაციაზე, გარდა სასამართლოს გადაწყვეტილების არსებობის შემთხვევისა. ქვემოთ აღწერილი ფიზიკური უსაფრთხოების სექცია უფრო დეტალურად აღწერს თუ როგორ ვიცავთ შენობის ფიზიკურ უსაფრთხოებას.

არაავტორიზებული ელექტრონული წვდომის თავიდან ასაცილებლად ჩვენ ვიყენებთ მოწინავე ქსელურ მოწყობილობებს, ცენტრალურ ანტივირუსულ პროგრამულ უზრუნველყოფას, ცენტრალურ განახლებების სისტემასა და ქსელური ინფორმაციის ფილტრს. ჩვენ რეგულარულად ვახდენთ რისკების შეფასებას და ჩვენი თანამშრომელია მგს 27001:2011 სერტიფიცირებული ინფორმაციული ტექნოლოგიებისა და ინფორმაციული უსაფრთხოების უფროსი.

<u>მთლიანობა</u> გულისხმობს ინფორმაციის შეუსაბამოდ შეცვლისგან დაცვას. კონფიდენციალობის მსგავსად, ჩვენ რეგულარულად ვახორციელებთ მომხმარებლების უფლებების გადახედვას, რაც საშუალებას გვაძლევს ინფორმაციის ცვლილების უფლება მივანიჭოთ მხოლოდ იმ თანამშრომლებს, ვისაც ეს ნამდვილად სჭირდებათ. ასევე, ჩვენს სისტემაში ვინახავთ აუდიტის ჟურნალს ყოველი განხორციელებული ქმედებისთვის და ამ აღრიცხვის ჟურნალების გადახედვაც ხდება რეგულარულ რეჟიმში.

<u>ხელმისაწვდომობა</u> დასტასთვის ნიშნავს, რომ ჩვენი სერვისები ხელმისაწვდომია ყოველთვის, როდესაც ის კლიენტს სჭირდება, მიუხედავად ჩვენი აპარატურისა თუ პროგრამული უზრუნველყოფის უეცრად მწყობრიდან გამოსვლისა. ამისთვის, ჩვენ ვაკეთებთ სარეზერვო ასლებს ყოველდღიურად და საათში ერთხელ (ინფორმაციის ტიპის გათვალისწინებით), რომელიც მოიცავს ფაილებს, მონაცემთა ბაზებს, ქსელური მოწყობილობების კონფიგურაციის ფაილებსა და სერვერების სრულ ასლებს. მაქსიმალური ხელმისაწვდომობის უზრუნველსაყოფად ჩვენ ვინახავთ სარეზერვო ასლებს, როგორც ღრუბლოვან სერვისებზე, ასევე ჩვენს ლოკალურ და დაშორებულ სერვერებზე. ჩვენ გვაქვს დუბლირებული ქსელური და სერვერული ინფრასტრუქტურა, თუ ერთ-ერთი მოწყობილობა გამოვა მწყობრიდან, ეს არ იმოქმედებს ხელმისაწვდომობაზე. ჩვენ ასევე გვაქვს ინტერნეტის ორი დამოუკიდებელი წყარო სხვადასხვა მომწოდებლისგან. სარეზერვო ასლები მოწმდება რეგულარულად, რაც გარანტიას იძლევა, რომ საჭიროებისას მათი გამოყენება შესაძლებელი იქნება. ჩვენ გვაქვს კატასტროფისგან აღდგენის

გეგმა და მუდმივად მზად მყოფი დაშორებული ოფისი, რაც უზრუნველყოფს ოპერირების გაგრძელების საშუალებას კატასტროფის შემთხვევაშიც კი.

ფიზიკური უსაფრთხოება

დასტას გააჩნია 24 საათიანი მუდმივი მონიტორინგის სისტემა, ხანძრის ამომცნობი და დამხშობი ტექნოლოგია, შეღწევის საწინააღმდეგო, ელექტრონული წვდომის კონტროლისა და გარემოს საფრთხეებისგან დამცავი სისტემები.

24 საათიანი ვიდეო-მეთვალყურეობა - დასტას ჰყავს ფიზიკური უსაფრთხოების თანამშრომლები, რომლებიც რეგულარულად გადიან ტრენინგს. ვიზიტორების რეგისტრაციისა და ტერიტორიის პატრულირების გარდა, ისინი აწარმოებენ ვიდეო-მეთვალყურეობას მუდმივ რეჟიმში. ფიზიკური უსაფრთხოების თანამშრომლების საქმიანობა სისტემატურად კონტროლდება.

ვიდეო-მეთვალყურეობის სისტემა - დასტას გააჩნია ვიდეო-მეთვალყურეობის კამერები, რომლებიც სრულად ფარავენ პერიმეტრს, საწყობის ყველა შესასვლელ კარს და ყველა სამუშაო ოთახს ოფისში. ვიდეო-ჩანაწერი ინახება მინიმუმ ერთი თვის განმავლობაში, ხოლო დაცვის თანამშრომლები რეალურ დროში აკვირდებიან გამოსახულებას.

ხანძრის გამოვლენა და ჩახშობა - ხანძრით გამოწვეული ზიანის პრევენციისთვის მთავარია ადრეული გამოვლენა, ამისთვის დასტას მთელს შენობაში გააჩნია 200-ზე მეტი კვამლის დეტექტორი, რომელიც დაკავშირებულია ცენტრალურ ხანძარსაწინააღმდეგო სისტემასთან. თავის მხრივ, ეს სისტემა დაკავშირებულია გადაუდებელი დახმარების ცენტრთან. ცეცხლის ქრობისთვის შენობის გარეთ ჩვენ გვაქვს ჰიდრანტები და სახანძრო შლანგები, ცეცლმაქრები CO2-ით და ცეცხლმაქრები ფხვნილით, რომლებიც განლაგებულია მთელს ტერიტორიაზე.

შეღწევის საწინააღმდეგო ტექნოლოგია - ჩვენ ვიყენებთ ორი განსხვავებული დეტექტორის ტიპს იმისათვის, რომ შევძლოთ შეღწევის დადგენა: მოძრაობის დეტექტორები და მსხვრევის დეტექტორები. ეს დეტექტორები დაკავშირებულია ცენტრალურ პანელთან, რომელიც თავის მხრივ დაკავშირებულია გადაუდებელი დახმარების ცენტრთან.

ელექტრონული წვდომის კონტროლი - განსაზღვრულ ადგილებში შესვლის შეზღუდვისთვის გამოიყენება ელექტრონული წვდომის კონტროლის სისტემა. ეს ადგილებია ოპერირების ზონა, სადაც ხდება დოკუმენტების დამუშავება, საწყობი და სასერვერო ოთახი. თითოეულ სივრცეს გააჩნის საკუთარი წვდომის კონტროლის მოწყობილობა, ხოლო მინიჭებული უფლებების გადახედვა ხდება რეგულარულად.

სასერვერო ოთახისთვის გათვალისწინებულია წვდომის კონტროლის სისტემა ორმაგი იდენტიფიკაციის ფუნქციით. ავტორიზებულმა თანამშრომელმა სასერვერო ოთახში შესაღწევად უნდა გამოიყენოს როგორც პერსონალური ბეიჯი, ასევე მინიმუმ 6-ნიშნა კოდი.

გარემოს საფრთხეებისგან დაცვა - იმის უზრუნველსაყოფად, რომ არ მოხდეს დოკუმენტების დაზიანება, ჩვენ მივმართავთ გარკვეულ ღონისძიებებს. პირველ რიგში, ჩვენ არასოდეს ვინახავთ დოკუმენტებს იატაკზე, ხოლო თაროები განლაგებულია მინიმუმ 20 სმ-ით ზემოთ იატაკიდან. მეორე, ჩვენ გვაქვს მავნებლებთან ბრძოლის პროგრამა, რომლის მეშვეობითაც ვუზრუნველყოფთ დოკუმენტების მავნებლებისგან დაცვას. მესამე, დოკუმენტების საწყობში ჩვენ ვაკონტროლებთ

ტემპერატურას და სინესტეს, რათა თავიდან ავიცილოთ მათი დაზიანება. მეოთხე, ჩვენ რეგულარულად ვასუფთავებთ საწყობს მტვრისგან.