IT უსაფრთხოების პოლიტიკა

1.გამოყენებული ტერმინები

1.1 **კონფიდენციალური** - ამ დოკუმენტის მიზნებისათვის კონფიდენციალური ინფორმაციის ქვეშ მოიაზრება ნებისმიერი ინფორმაცია/დოკუმენტაცია (როგორც ტექნიკური, ფინანსური და იურიდიული მონაცემები, ასევე პერსონალური მონაცემები და სხვა ინფორმაცია, მათ შორის ისეთი ინფორმაცია, რომელიც შეიძლება გაგებულ იქნეს ისე, რომ კონკურენტს მიეცეს საქმიანი უპირატესობა კომპანიასთან მიმართებაში) რომლის გამჟღავნებამ შეიძლება საფრთხე (ფინანსური, რეპუტაციული და ა.შ.) შეუქმნას კომპანიას, მის თანამშრომლებს და მსმენელებს.
1.2 **საიდუმლო** - ინფორმაციის ქვეშ მოიაზრება ნებისმიერი კონფიდენციალური ინფორმაცია/დოკუმენტაცია, რომლის გამჟღავნებამ შეიძლება სერიოზული/შეუქცევადი საფრთხე შეუქმნას კომპანიას, მის თანამშრომლებს და მსმენელებს. ინფორმაციის კლასიფიცირება ხდება კომპანიის მმართველი კომიტეტის მიერ.
1.3 **კომპანია** - მოხსენიებულია **სასტუმრო ლა ქინთა ბაი ვინდჰემ ბათუმი (მის: ქ.ბათუმი, ადლიის ქ. 1)**
1.4 **Email** - ელექტრონული ფოსტა.
1.5 **IT ინფრასტრუქტურა** - მოიცავს ყველა მოწყობილობას რომლებიც საჭიროა ციფრული ინფორმაციის დასამუშავებლად, შესანახად, გასაგზავნად.
1.6 **VPN – Virtual Private Network** - ვირტუალური კერძო ქსელის დანიშნულებაა უსაფრთხო გვირაბის შექმნა 2 მოწყობილობას შორის, მაგალითად ნოუთბუქსა და კომპანიის სერვერს შორის, სადაც შესაძლებელი იქნება ნებისმიერი ინფორმაციის დაცულად გაცვლა.
1.7 **IPS - Intrusion Prevention System** - შეჭრის პრევენციის სისტემა. ეს სისტემა გამოიყენება კომპანიებში IT ქსელის და მოწყობილობების დასაცავად.
1.8 **AD – Active Directory** სისტემა შექმნილია კომპანია მაიკროსოფტის მიერ და მისი ძირითადი დანიშნულებაა კომპიუტერების მომხმარებლების ცენტრალური აღრიცხვა და მათი მართვა.
1.9 **Firewall** - აპარატურული ან პროგრამული უზრუნველყოფა, რომელიც ახორციელებს მასში შემავალი პაკეტებისა და ტრაფიკის კონტროლს და ფილტრაციას.
1.10 **WIFI** - ლოკალურ ქსელში უსადენო კავშირის დამყარების ტექნოლოგია.
1.11 **Penetration Test** - IT სისტემებში არასანქცირებული შეღწევის ტესტირება.

2. ზოგადი დებულებები

2.1 წინამდებარე დოკუმენტი განსაზღვრავს ინფორმაციული ტექნოლოგიების მართვის პოლიტიკას, ინფორმაციული ტექნოლოგიების მართვის პროცედურებს, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურისა და უსაფრთხოების ნორმებს.
2.2 დოკუმენტში აღწერილი ნორმების დაცვა სავალდებულოა ყველა იმ პირისთვის, ვინც მუშაობს კომპანიაში და გაფორმებულია შრომითი ხელშეკრულება.
2.3 კომპანიის თანამშრომლები ვალდებულები არიან ამ დოკუმენტში აღწერილი IT უსაფრთხოების წესების დაცვის გარდა დაიცვან საქართველოს კანონმდებლობით დადგენილი მოთხოვნები ინტელექტუალური საკუთრების, ინფორმაციული ტექნოლოგიების უსაფრთხოებისა და პერსონალური ინფორმაციის დაცვასთან დაკავშირებით.
2.4 ამ დოკუმენტით განსაზღვრული წესების დარღვევის/შეუსრულებლობის შემთხვევაში თანამშრომელს დაეკისრება დისციპლინური პასუხისმგებლობის ზომა კომპანიისთვის მიყენებული ზიანის პროპორციულად.
2.5 პერსონალური მონაცემების დამუშავების, დაცვისა და უსაფრთხოების დეტალური წესები რეგულირდება კომპანიაში დამტკიცებული „პერსონალურ მონაცემთა დაცვის პოლიტიკით“.

3. ინფორმაციული ტექნოლოგიების მართვის პოლიტიკის ამოცანები

3.1 ინფორმაციული უსაფრთხოების პოლიტიკა უზრუნველყოფს კომპანიაში IT უსაფრთხოების კონტროლის მექანიზმების შექმნას რომელმაც უნდა უზრუნველყოს შესაძლო IT საფრთხეებისგან კომპანიის დაცვა. შესაძლო საფრთხეები შეიძლება იყოს:

- ჰაკერული შეტევა კომპანიის IT რესურსებზე.
- კომპიუტერული ვირუსის შეღწევა და გავრცელება კომპანიის ქსელში.
- კონფიდენციალური ან საიდუმლო ინფორმაციის დაკარგვა, მათი არასანქცირებულ პირთა ხელში მოხვედრა.

3.2 პოლიტიკა განსაზღვრავს:

- კომპანიის დაცულობას ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის თვალსაზრისით;
- პასუხისმგებლობებს ინფორმაციულ უსაფრთხოებაზე.

3.3 IT პოლიტიკის განმახორციელებლები, რაც მოიცავს სხვადასხვა IT სისტემების დანერგვას, მათ მართვას, ყოველდღიურ მონიტორინგს და ტექნიკურ მხარდაჭერას, არიან:

- IT სპეციალისტები.

4. პასუხისმგებლობა

პასუხისმგებლობები წინამდებარე პროცესის ფარგლებში შემდეგნაირად ნაწილდება:

დავალება	დირექტორი	IT სპეციალისტი	დასაქმებულები	საწყობის სპეციალისტი
სხვადასხვა IT სისტემების დანერგვა, მათი ყოველდღიური მართვა, მონიტორინგი, ტექნიკური მხარდაჭერა		✓		
IT მოწყობილობების ინვენტარიცაზია				✓
ცენტრალურ სერვერზე დაშვების დონეების განსაზღვრა თანამშრომლებისათვის	✓			
შეღწევის საწინააღმდეგო ტესტის ჩატარების უზრუნველყოფა		✓		
ინფორმაციული უსაფრთხოების ინციდენტების მართვა		✓		
თანამშრომელზე გადაცემული ინფორმაციის დაცულობა			✓	

5. ფიზიკური უსაფრთხოება

5.1 IT ცენტრალური მოწყობილობები (სერვერები, კომუტატორები, მარშუტიზატორი, Firewall) განთავსებულია **სპეციალურ სასერვერო ოთახში** (მის: ქ.ბათუმი, ადლიის ქ. 1) რომელიც ემსახურება სერვერებს ხოლო კომპანიისთვის საჭირო მოწყობილობები განთავსებულია ოფისშივე დაცულ ე.წ. ტექნიკურ ოთახში. მასთან წვდომა აქვთ მხოლოდ ავტორიზებულ პირებს:

- IT სპეციალისტებს.
- შესაბამისი დაშვების მქონე პირებს. (საზღვრავს დირექტორი)

5.2 პორტაბელური მოწყობილობების (ნოუთბუქები, USB მეხსიერების ბარათები და ა.შ. რომლებიც ინახავს ან ამუშავებს კომპანიისთვის მაღალი კრიტიკულობის, საიდუმლო ან კონფიდენციალურ მონაცემებს) ფიზიკურ უსაფრთხოებაზე პასუხისმგებლები არიან კომპანიის ის თანამშრომლები რომლებსაც აბარიათ ის კონკრეტული მოწყობილობა.

5.3 სავალდებულოა კომპიუტერული სისტემებისა და ქსელების დაცულობის უზრუნველყოფა ფიზიკური, ტექნიკური, პროცედურული და გარემოს უსაფრთხოების კონტროლის მექანიზმებით.

5.4 სერვერებზე, როუტერებზე, სვიჩებზე და ფაირვოლებზე ჩართულია მონიტორინგის და ლოგირების სისტემა. ინფორმაცია ინახება ცალკე სერვერზე და ხდება ამ ინფორმაციის სისტემატური მონიტორინგი. ინციდენტების შემთხვევაში ხდება მათზე რეაგირება.

6. პროგრამული უზრუნველყოფის გამოყენება

6.1 კომპანიაში ყველა IT პროგრამული უზრუნველყოფა ლიცენზირებულია მწარმოებლის მიერ.

6.2 ყველა კომპიუტერში უნდა იყოს ანტივირუსი.

6.3 ყველა პროგრამული უზრუნველყოფა (ოპერაციული სისტემები, ანტივირუსები) უნდა იყოს ყოველთვის განახლებული.

6.4 პროგრამული უზრუნველყოფების ლიცენზირებაზე პასუხისმგებელია **IT სპეციალისტი.** ნებისმიერი პროგრამული უზრუნველყოფის შეძენა უნდა მოხდეს მისი ჩართულობით.

7. კომპანიის კრიტიკული ინფორმაციის მატარებლები

7.1 კომპანიის ყველა IT სისტემის მენეჯმენტი შეზღუდულია, მასზე წვდომა აქვთ მხოლოდ იმ თანამშრომლებს, რომლებიც პასუხისმგებლები არიან სისტემის გამართულ ფუნქციონირებაზე.

7.2 ციფრული ინფორმაცია რომელიც კომპანიის ფუნქციონირებისთვის კრიტიკულია ინახება დუბლირებულ სერვერზე, რომელიც დუბლირებულია - ყოველდღიურად ხდება სხვა სერვერზე ფაილების რეზერვირება.

8. პერსონალური კომპიუტერი და ცენტრალური სერვერი

8.1 კომპანიის ყველა კომპიუტერი ჩართულია კორპორატიულ სისტემაში.

8.2 თითოეული თანამშრომლის მომხმარებელი შეზღუდულია. აკრძალულია პროგრამული უზრუნველყოფების ინსტალაცია ადმინისტრატორის გარეშე. ლოკალური ადმინისტრატორის უფლება შეიძლება ჰქონდეთ ინჟინრებს.

8.3 მომხმარებლის პაროლი უნდა შედგებოდეს მინიმუმ **8 (რვა) სიმბოლოსგან** და შეიცავდეს ციფრებს, ასოებს, სიმბოლოებს.

8.4 ფაილ სერვერზე დაშვება ხდება დეპარტამენტების მიხედვით. დეპარტამენტის ხელმძღვანელის მიერ წარმოდგენილ სტრუქტურაში განსაზღვრულია თუ ვის რა ტიპის წვდომა აქვს და რომელ ფაილზე. ეს ინფორმაცია შეთანხმებულია კომპანიის დირექტორთან. IT სპეციალისტი ტექნიკურად ასრულებს წვდომების გაწერას სისტემაში. სტრუქტურის განახლება ან შეზღუდვების ცვლილება ხდება მხოლოდ დეპარტამენტის ხელმძღვანელის მითითების საფუძველზე. მითითება უნდა იყოს წერილობითი.

9. ინფორმაციული უსაფრთხოების ინციდენტები

9.1 კომპანია ახორციელებს უსაფრთხოების ინციდენტების იდენტიფიცირებას, რაც ასევე გულისხმობს თითოეული ინციდენტის შესწავლას, აღწერასა და მათზე ადეკვატურ რეაგირებას. ინციდენტებზე რეაგირებაზე პასუხისმგებელია **IT სპეციალისტი.**

9.2 IT რისკების შეფასება კომპანიის ერთიანი რისკების შეფასების ნაწილია, რომელიც გადაიხედება და განახლდება ყოველწლიურად.

9.3 იმ შემთხვევაში, თუ ინფორმაციული უსაფრთხოების ინციდენტი შეიცავს პერსონალური მონაცემების უსაფრთხოების დარღვევის (გაჟონვა, დაკარგვა, არასანქცირებული წვდომა) ნიშნებს, მასზე რეაგირება და შესაბამისი უწყების/სუბიექტის ინფორმირება ხორციელდება კომპანიის „ინციდენტების მართვის პროცედურის“ შესაბამისად.

10. კონფიდენციალურ და საიდუმლო ინფორმაციასთან მოქცევის წესები

10.1 აკრძალულია IT სისტემებისთვის განკუთვნილი მომხმარებლის იუზერების, პაროლების, პინების სხვისთვის განდობა.

10.2 აკრძალულია უცხო ინფორმაციის მატარებლების (USB Flash Drive, USB HDD) კომპიუტერებში და სხვა IT სისტემაში მიერთება. გამონაკლისი შეიძლება იმ შემთხვევაში, თუ უცხო ინფორმაციის მატარებელს შეამოწმებს IT სპეციალისტი.

10.3 კონფიდენციალური ინფორმაციის გაზიარება უნდა მოხდეს მხოლოდ წვდომის უფლების მქონე პირებზე.

10.4 არ გამოიყენოთ პერსონალური მესენჯერები ან Email-ი კომპანიასთან დაკავშირებით. აკრძალულია მათი მეშვეობით კონფიდენციალური ინფორმაციის გაცვლა.

10.5 სამუშაო ადგილი და პერსონალური კომპიუტერის ეკრანი გქონდეთ მოწესრიგებული, რათა არ მოხდეს კონფიდენციალური ინფორმაციის ნახვა არაავტორიზირებული პირის მხრიდან.

10.6 პერსონალური მონაცემების შენახვის ვადები, მათი სისტემებიდან უსაფრთხოდ წაშლა/განადგურება და მონაცემთა მინიმიზაციის წესები განისაზღვრება კომპანიაში დამტკიცებული „პერსონალურ მონაცემთა დაცვის პოლიტიკით“.