Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi
Məlumat Hesablama Mərkəzi

Qeyd.№ _____

Təsdiq edirəm
Direktor
_____E. Əsədov
"02" Mart 2019-cu il

Nəqliyyat,Rabitə və Yüksək Texnoloqiyalar Nazirliyinin Məlumat Hesablama Mərkəzi

	Nəşr tarixi: 02.03.2019
Məlumat Hesablama Mərkəzində İnformasiya Təhlükəsizliyini İdarəetmə Siyasəti	Səhifə, cəmi: 6

Hazırladı			Razılaşdırıldı		
Adı	İmza	Tarix	Adı	İmza	Tarix
İTŞ-in müdiri Rahib Ağababayev			*Informasiya Təhlükəsizliyi üzrə ekspert Murad Qurbanov*		

Versiya	Tarix	Səbəb	Dəyişiklik edən şəxs
1.0	Yanvar, 2019	İlk versiyanın nəşri	Rahib Ağababayev

Sənədin müəllifi:

Sahibi	Müəllif	Tərtib tarixi
Məlumat Hesablama Mərkəzi	Rahib Ağababayev	Yanvar 2019

Sənədin yayınlanma sahəsi:

Məlumat Hesablama Mərkəzi daxilində istifadə üçün

1. Ümumi müddəalar

1.1. "Məlumat Hesablama Mərkəzində (bundan sonra – MHM-də) informasiya təhlükəsizliyini idarəetmə Siyasəti" (bundan sonra – Siyasət) informasiya təhlükəsizliyini idarəetmə sistemi (bundan sonra – İTİS) üçün MHM-də rəhbərlik tərəfindən rəsmi ifadə olunan məqsəd və hədəfləri ümumən müəyyən edir;

1.2. Bu məqsəd və istiqamətlər MHM-in xidməti fəaliyyətinin prioritetlərinə, bu fəaliyyəti nizamlayan normativ hüqiqi və texniki aktların (Əlavə №1) tələblərinə, o cümlədən həmin fəaliyyətin proses və xüsusiyyətlərinə uyğun olmalıdır;

1.3. Bu Siyasət ISO/IEC-27001 *("İnformasiya Təhlükəsizliyi. Təhlükəsizlik metodları.İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Tələblər")* beynəlxalq standartın tətbiqi məqsədi ilə hazırlanmışdır, İTİS-in sənədlər toplusuna daxildir;

1.4. Bu Siyasətdə MHM rəhbərliyinin İTİS-ə aid vəzifələrini və MHM-in bu sistemə yanaşmasını ifadə edilir;

1.5. Siyasət MHM-in bütün əməkdaşları və bağlanmış müqavilələr çərçivəsində MHM-in məlumatları ilə işləyən şəxslərə şamil edilir;

1.6. Bu Siyasətin adekvatlığını və effektivliyini təmin etmək üçün ona, plan üzrə müəyyən edilmiş müddətlər başa çatanda və ya əhəmiyyətli dəyişikliklərə zərurət yarananda, vaxtaşırı yenidən baxılmalıdır;

2. Normativ tələblərə uyğunluq

2.1. MHM-in İTİS üzrə fəaliyyəti Azərbaycan Respublikasının normativ hüquqi aktlarında (Əlavə №1, I hissə) nəzərdə tutulmuş müddəalarla yanaşı, informasiya təhlükəsizliyi sahəsində milli və beynəlxalq standartlara (Əlavə №1, II hissə), MHM-in daxili normativ sənədlərinə (Əlavə №1, III hissə) əsaslanır;

2.2. İTİS üçün həmçinin bu sahənin tənzimlənməsində iştirak edən qurumların tövsiyyələrindən, bu sahədə beynəlxalq və milli təcrübənin nəticələrindən istifadə olunur.

3. İnformasiya təhlükəsizliyinə dair minimal tələblər

3.1 İnformasiya təhlükəsizliyi və məlumatların qorunması dedikdə məlumatların məxfiliyinin, tamlığının və mövcudluğunun təmin edilməsi nəzərdə tutulur. Məxfilik – informasiyanın icazəsiz əldə olunmasına məhdudiyyət qoyulmasını;Tamlıq – informasiyanın əvvəlcədən müəyyən edilmiş şəkil və keyfiyyəti saxlamasını, dəqiqliyini və mötəbərliyini; Əlyetənlilik – yol verilən

vaxt ərzində tələb olunan informasiya resursunu, informasiya xidmətini əldə etmək imkanını ifadə edir;

3.2 İnformasiya təhlükəsizliyinin təmin edilməsi informasiya təhlükəsizliyi risklərinin reallaşması səbəbindən dəyəcək zərərin minimallaşdırılması, korporativ informasiya təhlükəsizliyi mədəniyyətinin və reputasiyasının yaxşılaşdırılması məqsədi daşıyır;

3.3 İnformasiya vacib aktiv hesab edilməlidir və onun qorunması hər əməkdaşın məsuliyyətidir;

3.4 İşçilərə və mülki hüquq müqaviləsi əsasında xidmət göstərən heyətə (bundan sonra - kontraktorlar) korporativ informasiyaya buraxılışlar vəzifə\müqavilə öhdəliklərini yerinə yetirməsini təmin edəcək həcmdə təqdim edilməlidir;

3.5 Yeni təhdid mexanizmlərinin yaranması səbəbindən İTİS davamlı olaraq təkmilləşdirilməli, informasiya təhlükəsizliyi üzrə siyasətlər, qaydalar, prosedurlar və digər normativ sənədlər müntəzəm olaraq optimallaşdırılmalı, qanunvericiliklə uyğunlaşdırılmalıdırlar;

3.6 İcazəsiz fəaliyyətin qarşısını almaq üçün bütün kritik və həssas İT avadanlıqların fiziki təhlükəsizliyi təmin edilməlidir;

3.7 İstifadəçilər fəaliyyətlərinə görə məsuliyyət daşıyır və onların fəaliyyətinə nəzarət mexanizmləri tətbiq edilməlidir;

3.8 Portativ qurğularda saxlanılan məlumatların təhlükəsizliyi təmin edilməlidir;

3.9 Bütün İT sistemlər beynəlxalq təcrübələrə,daxili qaydalara və qanunvericiliyə uyğun konfiqurasiya edilməlidir;

3.10 İnsidentlərin cavablandırılması prosesi mövcud olmalı və insidenlərin sənədləşməsi qaydaları tərtib edilməlidir;

3.11 Kompüter şəbəkəsinə icazə verilməmiş avadanlıq və cihazların qoşulması qadağandır;

3.12 Konfidensial və xüsusi məlumatlar təhlükəsiz kanallarla ötürülməlidir;

3.13 Əməkdaşların İnternet çıxışlarına iş davamlılığına zərər gətirmədən limitlər tətbiq edilməli və nəzarət edilməlidir;

3.14 Hər informasiya resursunun bu resursa buraxılışların verilməsini və effektiv istifadəsini təmin edən nəzarətçisi təyin edilməlidir;

3.15 Əməkdaşlar müntəzəm olaraq informasiya təhlükəsizliyi təlimlərində iştirak etməlidirlər;

3.16 Hər il müstəqil informasiya təhlükəsizliyi auditi keçirilməlidir;

3.17 İnformasiya təhlükəsizliyi şöbəsi informasiya təhlükəsizliyi üzrə tələblərin müəyyən edilməsinə və tələblərin icrasına nəzarət edilməsinə cavabdehdir;

3.18 İnformasiyanın qorunması və informasiya təhlükəsizliyi üzrə tədbirlər risklərin qiymətləndirilməsi prosesinin nəticələri əsasında həyata keçirilir;

3.19 İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi illik olaraq, yeni layihələrin və proseslərin tətbiqi zamanı həyata keçirilir;

3.20 Risklərin qiymətləndirilməsi zamanı informasiya təhlükəsizliyi risklərinin reallaşmasının MHM-in maliyyə və nüfuzuna təsirləri nəzərə alınmalıdır;

3.21 İnformasiya təhlükəsizliyi tədbirlərinin dəyəri təhdidlərin reallaşması zamanı potensial olaraq dəyə biləcək zərərdən yüksək olmamalıdır.

4. Məsuliyyətlər

4.1 MHM -in işçiləri və kontraktorları onların vəzifəsindən və statusundan asılı olmayaraq bu siyasətə riayət etmək üçün məsuliyyət daşıyırlar;

4.2 İşçiləri və kontraktorları tərəfindən informasiya təhlükəsizliyi siyasətinə riayət edilməməsi qanunvericiliyə uyğun məsuliyyət tədbirlərinin tətbiq edilməsi üçün əsasdır.

"İnformasiya təhlükəsizliyini idarəetmə Siyasəti"nə
Əlavə №1

I. İTİS üçün istinad olunan normativ hüquqi aktlar:	
1	Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu və onun tətbiqinə aid normativ aktlar
2	Azərbaycan Respublikasının "Elektron imza və elektron sənəd haqqında" Qanunu
3	Azərbaycan Respublikasının "Fərdi məlumatlar haqqında" və "Biometrik informasiya haqqında"Qanunları, onların tətbiqinə aid normativ aktlar
4	Azərbaycan Respublikasının "Biometrik informasiya haqqında" Qanunu
5	Azərbaycan Respublikasının "Kommersiya sirri haqqında" Qanunu
6	Azərbaycan Respublikasının "Telekommunikasiya haqqında" və "Poçt rabitəsi haqqında" Qanunları
7	Azərbaycan Respublikasının "Müəlliflik hüquqlarının qorunması" Qanunu
8	"Dövlət hakimiyyəti orqanlarında, idarə, təşkilat və müəssisələrində kargüzarlığın aparılmasına dair Təlimat" (Azərbaycan Respublikası Prezidentinin Fərmanı – № 935, 27.09.2003-cü il)
9	
10	
	II. İTİS üçün istinad olunan normativ hüquqi texniki aktlar (standartlar):
1	ISO/IEC 27001 "Information technology - Security techniques - Information security management systems – Requirements"
2	ISO/IEC 27002 "Information technology - Security techniques - Code of practice for information security management"
3	ISO/IEC 15408 " "
4	ISO/IEC 12207 " "
5	ISO 22301 "Societal security - Business continuity management systems – Requirements"
6	ISO/IEC 20000 "Information technology - Service management"
7	ISO 9001 "Quality management systems – Requirements"
8	ISO 19011 "Guidelines for quality and/or environmental management systems auditing"
9	
	III. İTİS üçün istinad olunan daxili normativ sənədlər:
1	İnformasiya prosesləri və texnologiyaları ilə iş proseslərində təhlükəsizliyin təmin olunmasına dair Metodik Göstərişlər
2	Ehtiyat nüsxələmə və verilənlərin bərpası siyasəti
3	Dəyişikliklərin idarəedilməsi və nəzarət olunması siyasəti
4	Şifrə siyasəti
5	İnsidentlərin İdarəedilməsi Qaydaları
6	Dəyişikliklərin idarə edilməsi və nəzarət edilməsi siyasəti