*Nümunəvi Təlimat layihəsi*

**Azərbaycan Respublikasının müvafiq dövlət qurumunda informasiya təhlükəsizliyinin təmini üzrə**

**T Ə L İ M A T**

1. **Ümumi müddəalar**
   1. Bu təlimat Azərbaycan Respublikası müvafiq dövlət qurumunda informasiya təhlükəsizliyinin təmin edilməsi, o cümlədən korporativ informasiya məkanında potensial təhdidlərə qarşı qabaqlayıcı və təshihedici tədbirlərin müəyyən olunması məqsədi ilə hazırlanmışdır.
   2. Bu Təlimat Azərbaycan Respublikası müvafiq dövlət qurumunda informasiya təhlükəsizliyinin təşkili və təmini qaydalarını, habelə struktur bölmələr və əməkdaşlar üçün informasiya təhlükəsizliyi sahəsində məcburi tələbləri müəyyən edir.
2. **Əsas anlayışlar**
   1. **İnformasiya təhlükəsizliyi –**informasiya **İnformasiya təhlükəsizliyi -**informasiyanın tamlıq, əlçatarlıq, konfidensiallıq xassələrinin və ona xidmət edən infrastrukturun məqbul yetərlilik və yararlılıq hədlərinin təmin edilmə, bu informasiyaya və ona xidmət edən infrastrukturun sahibinə və ya istifadəçilərinə ziyan vurmağa səbəb ola bilən təbii və ya süni xarakterli təsadüfi baş verən və ya qəsdən törədilən təsirlərdən mühafizəli olunma halıdır.
   2. **Məxfi məlumat -** dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən, məlumat daşıyıcısının özündə və ya ona qoşulan sənədlərdə məxfilik qrifi qoyulan və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlardır.
   3. **Konfidensial informasiya -** vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə olunmasına məhdudiyyət qoyulan məlumatları, o cümlədən fərdi məlumatları, habelə peşə (həkim, vəkil, notariat və s.), kommersiya, istintaq və məhkəmə sirləri və s. olan informasiyadır.
   4. **HTTPS protokol –** istifadəçilər ilə server arasında xüsusi tunelin yaradılması ilə istifadəçi trafikini 3-cü tərəflərin dinləməsindən/müdaxiləsindən qoruyan “SSL” şifrləmə protokulu ilə təchiz olunmuş şifrləmə mexanizmidir.
   5. **VPN xidmət –** trafikin 3-cü tərəflərin dinləməsindən/müdaxiləsindən qorunmaqla xüsusi tunel vasitəsi ilə ötürülməsinin təmin edilməsidir.
   6. **Xidmət sahəsi –** əməkdaşın xidməti fəaliyyətini həyata keçirdiyi məkandır (yerdir).
   7. **P2P –** mərkəzi server olmadan bir-birinə ötürməyə imkan verən şəbəkə protokoludur.
   8. **Qoruyucu divar (“firewall”)** - Internetdən gələn təhlükələrə qarşı müdafiə üçün informasiya sisteminə və şəbəkəyə girişi məhdudlaşdıran və ya əngəlləyən təhlükəsizlik sistemidir.
   9. **Qısaldımış, dəyişdirilmiş keçid –** uzun keçidlərin (URL) göndərilməsini və yadda saxlanılmasını asanlaşdırmaq məqsədilə onların qısaldımasıdır (Qeyd: Hakerlər bu metoddan saxta və zərərli keçidlərin əsl adlarının gizlətmək (dəyişdirmək) məqsədi ilə istifadə edir. Nümunə: bit.ly, tiny.url, goo.gl və s.).
   10. **Dayanıqlı şifrə** (*“password”*, keçərsöz) **-** böyük hərf, kiçik hərf, simvol və rəqəmlərdən ibarət olan və 10 simvoldan az olmayan şifrə (Qeyd: Dayanıqlı şifrələr aşağıdakı informasiya resursundan istifadə edilməklə hazırlana bilər: <https://cert.gov.az/az/password-generator>).
   11. **Simsiz texnologiya** - bluetooth, infrared, simsiz kompüterlər və periferiya qurğuları (printer, klaviatura, mouse, ağıllı saat, simsiz qulaqcıq və s.), həmçinin ağıllı avadanlıqlar kimi soyuducular və s. simsiz texnologiyalar hesab olunur.
   12. **Ransomware** – faylların və ya kompüterin şifrlənməsi yolu ilə zədələnmiş və ya şifrlənmiş faylların bərpası üçün ödəniş tələb edən zərərverici proqram vasitələrinin xüsusi növüdür.
   13. **Sosial mühəndislik –** xüsusi bilik və texniki vasitələrdən istifadə etmədən insanların manipulyasiya edilməsi, aldadılması və ya danışdırılması yolu ilə məxfi, konfidensial, o cümlədən fərdi, həmçinin xidməti məlumatların əldə olunması metodudur. (Qeyd: Sosial mühəndislik daha çox telefon zəngi ilə anketlərin doldurulması (bank və sığorta şirkətlərinin, digər subyektlərin adından istifadə olunmaqla gələn zənglər ola bilər), e-mail vasitəsilə daxil olan elektron formaların doldurulması və ya hədəfin hansısa mövzu ətrafında fikir mübadiləsinə cəlb edilməsi yolu ilə həyata keçirilir).
   14. **Ağıllı mobil telefon –** istifadəçilər tərəfindən proqram tətbiqlərinin yazılmasını mümkün edən Android, İOS, Windows, Blackberry və digər əməliyyat sistemlərinə malik mobil qurğudur.
   15. **Fərdi məlumat -** fiziki şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatdır.
3. **İnformasiyanın mühafizəsi ilə bağlı qadağalar**
   1. Məxfi və ya konfidensial məlumatı icazəsiz əldə etmək və ya ələ keçirmək;
   2. Əməkdaşın xidməti istifadəsi üçün zəruri olmayan məxfi, konfidensial məlumatla tanış olmaq, məlumatı əldə etmək, saxlamaq və ya digər məqsədlər üçün istifadə etmək;
   3. Buraxılışına xüsusi nəzarət olunan, elektron avadanlıqların istifadəsi qadağan olunmuş ərazilərə ağıllı mobil telefon, kompüter, və s. kimi elektron avadanlıqlarla daxil olmaq;
   4. Məxfi və ya konfidensial informasiyanı qeydiyyata alınmamış informasiya daşıyıcılarında[[1]](#footnote-2) saxlamaq;
   5. Məxfi məlumatı məxfiləşdirilmiş şəbəkədən və ya kompüterdən yaddaş ötürücülərinə icazəsiz yazmaq;
   6. Məxfi, konfidensial və ya xidməti informasiyanı təhlükəsizlik səviyyəsi və kanalları müəyyən edilməmiş faks aparatları ilə göndərmək;
   7. Məxfi şəbəkəyə qoşulmuş, eləcə də məxfi sənədlər hazırlanan kompüterləri və digər qurğuları hər hansı internet bağlantısı olan şəbəkəyə qoşmaq;
   8. Məxfi şəbəkədən internet bağlantısı olan kompüterə və ya əksinə məlumat köçürmək;
   9. Məxfiləşdirilmiş şəbəkə avadanlığını açıq və daha aşağı səviyyəli şəbəkəyə qoşmaq;
   10. Xidməti istifadə üçün təhkim olunmuş avadanlığı təyinatından kənar, o cümlədən şəxsi məqsədlər üçün istifadə etmək.
4. **Rabitə vasitələrindən istifadə qaydaları**
   1. Təhkim olunmuş rabitə vasitələrindən yalnız xidməti məqsədlər üçün istifadə edilməlidir;
   2. Təhkim olunmuş rabitə vasitələri hər bir əməkdaşın şəxsi inventar kartında qeydə alınmalı və xidmətin sonunda təhvil götürülməlidir;
   3. Xüsusi dövlət rabitəsindən yalnız xüsusi dövlət rabitəsi ilə təmin olunan vəzifəli şəxslər istifadə etməlidir;
   4. Rabitə xətlərini icazəsiz konsentratorlar və ya başqa kommutasiyalı qurğulara qoşmaq, həmçinin telefon aparatına cütləşmə və ya xüsusi keçirmə açarı ilə əlavə telefon aparatı qoşmaq qadağandır;
   5. Xüsusi şifrləmə ilə təmin olunmamış rabitə vasitələrilə məxfi danışıqlar aparmaq qadağandır;
   6. Xidməti, konfidensial və ya məxfi danışıqları rabitə vasitəsinin “ucadan danışma” (“speaker”) funksiyasından istifadə etməklə aparmaq qadağandır;
   7. Xidməti rabitə vasitələrində olan ölkədaxili və beynəlxalq danışıq limitlərindən şəxsi məqsədlər üçün istifadə etmək qadağandır;
   8. “Xüsusi rabitə çağırışları” təhkim olunmuş şəxslər tərəfindən ciddi qorunmalıdır;
   9. Rabitə kanalları yalnız xidməti istifadəyə zəruri olan kanal sayı ilə, minimum imtiyaz siyasəti ilə təchiz edilməlidir;
   10. Təhkim olunmuş rabitə vasitəsini müvəqqəti istifadə üçün və ya saxlamaq üçün digər şəxsə vermək və ya söndürmək qadağandır;
   11. Rabitə vasitələrinin düzgün istifadəsi daima nəzarətdə saxlanılmalı və pozuntu halları aktlaşdırılmalıdır;
   12. Rabitə vasitəsinin itirilməsi, 3-cü şəxslər tərəfindən ələ keçirilməsi və s. kimi neqativ hallarda dərhal müvafiq struktur bölməyə və onun vasitəsilə müvafiq quruma dərhal məlumat verilməlidir.
5. **Kompüterdən istifadə qaydaları**
   1. Təhkim olunan kompüterdən xidməti zərurətdən kənar məqsədlə istifadə etmək qadağandır;
   2. Şəxsi məlumatların təhkim olunan kompüterə köçürülməsi qadağandır;
   3. Təhkim olunmuş kompüterin konfiqurasiyalarına (reyestr, idarəetmə paneli, sistem faylları və s.) istifadəçi tərəfindən müdaxilə etmək qadağandır. (Qeyd: Kompüterin konfiqurasiyasında dəyişiklik texniki qulluğa səlahiyyəti olan struktur bölmə, mütəxəssis, qurum tərəfindən aparılır. Bunun üçün müraciət, icazə və ya imtina, dəyişiklik və onun nəticəsi barədə informasiya mübadiləsi “ServiceDesk” jurnalı vasitəsilə aparılmalı və qeydiyyata alınmalıdır.)
   4. Şəxsi istifadədə olan “USB” avadanlıqlarını (mobil telefon, kofe isidici, sərinkeş və s.) təhkim olunmuş kompüterə hər hansı məqsəd üçün (istifadə və ya enerji toplanması üçün) qoşmaq qadağandır;
   5. Kompüter lisenziyalı əməliyyat sistemi və digər lisenziyalı proqram təminatları ilə təchiz edilməlidir;
   6. Qanuna zidd və lisenziyasız proqram təminatlarının kompüterdə istifadəsi qadağandır;
   7. Kompüterin əməliyyat sisteminə məxsus yenilənmələr (“update”) müvafiq qaydada, o cümlədən səlahiyyətli struktur bölmənin inzibatçılığı ilə və mütəmadi şəkildə həyata keçirilməli və əməliyyat sisteminin yenilənmələr (“update”) funkisyası aktiv saxlanılmalıdır;
   8. Kompüter, o cümlədən istifadə olunan digər informasiya sistemləri lisenziyalı antivirus proqram təminatı ilə təchiz olunaraq mərkəzləşdirilmiş antivirus sisteminə qoşulmalı və daima yenilənməsi təmin olunmalıdır;
   9. Kompüterlər, informasiya daşıyıcıları mütəmadi olaraq antivirus proqramları vasitəsilə yoxlanılmalıdır (“scanning”);
   10. Kompüterin təhlükəsizlik divarı (“firewall” müdafiəsi) daima aktiv olmalıdır;
   11. İstifadə edilən kompüterin qarşısından uzaqlaşan zaman ekran kilid vəziyyətinə keçirilməlidir və kilid vəziyyəti dayanıqlı şifrə ilə təmin edilməlidir;
   12. Kompüterin zərərvericilərə, xüsusən də “Ransomware” virusuna yoluxması halında, zərərvericinin digər şəbəkə elementlərinə yayılmasının qarşısını almaq üçün həmin kompüter dərhal internet, habelə daxili şəbəkədən ayrılmalı və müvafiq şöbə məlumatlandırılmalıdır;
   13. Kompüterin “Ransomware” zərərvericisinə yoluxması halında, zədələnmiş faylların bərpası üçün haker tərəfindən tələb olunan ödənişin həyata keçirilməsi və ya hər hansı digər tələbin icrası yolverilməzdir;
   14. Kompüterlərin əməkdaşlara təhkim olunması, istifadələrinə verilməsi zamanı istifadəçinin xidməti fəaliyyətini təmin edəcək minimum imtiyazlı konfiqurasiya (yalnız xidməti istifadə üçün zəruri olan proqramların yazılması, portların bağlanması, inzibatçı səlahiyyətlərinin məhdudlaşdırılması və s.) təyin edilməlidir. Bu konfiqurasiyanın təyin edilmiş vəziyyətin monitorinq olunması, həmin vəziyyətdə dəyişmə hallarının dərhal aşkar olunması təmin edilməlidir.
6. **Daxili şəbəkə və internetdən istifadə qaydaları**
   1. “AzSateNet” (dövlət) şəbəkəsindən istifadə etməklə zərərverici proqram təminatlarını (“rootkit”, “troyan” və s.)[[2]](#footnote-3) yaymaq və ya digər bir istifadəçiyə göndərmək qadağandır;
   2. Qeydiyyata alınmamış və razılaşdırılmamış Wi-Fi qurğularını, o cümlədən “smart tv” və “smart tv box”-ları şəbəkəyə qoşmaq qadağandır;
   3. Razılaşdırılmamış8 “P2P” əlaqəsi istifadə edən sistem və tətbiqlərdən (“Torrent”, “Flashget”, “Tor” və s.), habelə xidmət üçün istifadəsi təsdiqlənməmiş VPN xidmətlərindən istifadə etmək qadağandır;
   4. Dövlət internet şəbəkəsindən və ya təhkim olunmuş kompüterdən istifadə etməklə şəbəkə oyunları (online/offline), qumar, idman mərc və “18+” kontentə malik informasiya resurslarından istifadə etmək qadağandır [[3]](#footnote-4);
   5. Xidməti istifadə üçün nəzərdə tutulmamış, icazə verilməmiş proqram təminatlarının (internetdən yükləməklə və ya hər hansı məlumat daşıyıcısından istifadə etməklə) təhkim olunmuş kompüterə quraşdırılması qadağandır;
   6. Zərərli kontentdən müdafiə məqsədi ilə bütün baxış proqramlarında (“browser”) <https://blacklist.gov.az> tətbiqi istifadə edilməlidir;
   7. Bank kartları ilə ödənişlər, elektron poçt ünvanlarına girişlər yalnız “HTTPS” protokolu aktiv olduğu zaman həyata keçirilməlidir;
   8. Xidməti tapşırıqların yerinə yetirilməsi üçün zərüri olan bütün proqram təminatları onların müvafiq cədvəl formasında siyahısı (o cümlədən cədvəlin strukturu) müvafiq struktur bölməsi ilə razılaşdırıldıqdan sonra qeydiyyata alınmaqla və yalnız həmin şöbənin tövsiyə etdiyi resurs və ya vasitələrdən istifadə edilməklə təhkim olunmuş kompüterə quraşdırılmalıdır;
   9. Dövlət internet şəbəkəsindən və ya təhkim olunmuş kompüterdən maddi mənfəət əldə etmək və ya digər məqsədlər üçün kompüterin əməliyyat gücündən, yaddaş və s. imkanlarından üçüncü tərəflərə istifadə səlahiyyəti verən sistem və ya tətbiqlərdən istifadə etmək qadağandır;
   10. Xidməti vəzifələrinə və işinə birbaşa aidiyyəti olmayan internet informasiya resurslarına daxil olmaq qadağandır;
   11. “URL qısaltma” (dəyişmə) xidmətlərindən istifadə edərək əsas domenini gizlədən informasiya resurslarından və ya keçidlərindən istifadə etmək qadağandır;
   12. Məlumatların dövlət qurumunun xidməti istifadəsi üçün nəzərdə tutulmamış bulud xidmətində (“google drive”, “office 365”, “dropbox”, “icloud”, “onedrive”, “boxca” və s.) saxlanılması qadağandır;
   13. Xidmət sahəsində, xidməti avadanlıqların kənar internet (“Mİ-Fİ”, “Data kart”, “ADSL”, “Mobile Hotspot” və s.) bağlantı vasitələrinə qoşulması qadağandır;
   14. Xidməti şəbəkədə qeydiyyata alınmayan və razılaşdırılmamış avadanlıqların istifadəsi aşkarlanarkən, bu avadanlıqlar aktlaşdırılaraq istifadədən kənarlaşdırılmalıdır.
7. **“Simsiz texnologiyanın” istifadəsi ilə bağlı qaydalar**
   1. Simsiz texnologiyadan istifadə edərkən həmin texnologiya vasitəsi ilə ötürüləcək məlumatın konfidensiallıq səviyyəsi müəyyən edilməlidir. (Qeyd: Bunun üçün məlumatların təsnifatlaşdırılması əvvəlcədən təmin edilməlidir);
   2. Xidmət sahəsində qeydiyyata alınmamış və razılaşdırılmamış simsiz texnologiyaların istifadəsi qadağandır;
   3. Daxili şəbəkəyə qoşulmuş bütün kompüter, periferiya və digər avadanlıqların ikinci simsiz əlaqə interfeysi söndürülməlidir;
   4. Simsiz rabitə ilə təchiz olunmuş printerlərin və bu kimi digər avadanlıqların istismarı zamanı “Wi-Fi” funksiyası söndürülməlidir;
   5. Daxili şəbəkəyə müdaxilə etmək imkanı yaratdığına görə bina xaricinə şəbəkəni çatdıran və razılaşdırılmamış yerlərdə “Wi-Fi” ötürücü və gücləndiricilərin daxili şəbəkəyə qoşulması qadağandır;
   6. Kompüterə simsiz, şifrlənməmiş, qeydiyyata alınmamış və razılaşdırılmamış11 periferiyaların (keyboard, mouse və s.) qoşulması qadağandır.
8. **Elektron poçt ünvanlarından istifadə və təhlükəsizlik qaydaları** 
   1. Xidməti istifadə üçün yalnız @qurumundomeni.gov.az elektron poçt ünvanından istifadə olunmalıdır;
   2. Xidməti və rəsmi yazışmalarda şəxsi elektron poçt ünvanından istifadə etmək qadağandır;
   3. Xidməti elektron poçt ünvanından istifadə etməklə xidməti fəaliyyətlə əlaqəsi olmayan məlumatlar və sənədlər göndərmək və ya onların yayılmasında iştirak etmək qadağandır;
   4. Kənar internet informasiya ehtiyatlarında qeydiyyat zamanı xidməti elektron poçt ünvanını istifadə etmək qadağandır (“hesab.az”, “turbo.az”, “facebook”, “google” və s.);
   5. Elektron poçt vasitəsi ilə naməlum şəxslər tərəfindən göndərilmiş sorğulara, linklərə keçid etmək və elektron poçta cavab vermək qadağandır[[4]](#footnote-5);
   6. Elektron poçt vasitəsi ilə vədverici məktubların (Pul uduşları, mükafatlandırmalar, əmanətin ötürülməsi, təyyarə bileti, bank hesabının açılması, pul köçürmə əməliyyatları, faktura ödənişi və s.) alınması zamanı həmin məktubdakı keçidlərə daxil olmadan (klik etmədən) və elektron poçta cavab vermədən şübhəli daxilolma barədə müvafiq şöbəyə məlumat verilməlidir;
   7. Elektron poçt və ya telefon zəngi vasitəsi ilə adların saxtalaşdırılması ilə hansısa əməkdaşın və ya struktur bölmənin adından göndərilən texniki əməliyyatlardan ibarət tapşırıqlar (poçt qutusu ilə bağlı əməliyyatlar, şifrlərin dəyişdirilməsi, elektron poçt həcminin artırılması, kompüterdə, bütün baxış proqramlarında (“browser”) və ya hansısa proqram təminatında yenilənməni tələb edən və s.) elektron poçtu göndərən tərəflə həmin tapşırığın saxta olub-olmadığı zəng və ya digər alternativ əlaqə vasitələri ilə yoxlanıldıqdan sonra icra olunmalıdır;
   8. Xidməti və konfidensial məlumatların yalnız və yalnız “gov.az” domen zonasında olan elektron poçt ünvanları arasında mübadiləsinə icazə verilir. Bu kimi məlumatların elektron poçtla göndərilən zaman xüsusi şifrləmə metodları ilə əlavə şirflənməsi tövsiyyə olunur;
   9. Elektron poçt və ya digər elektron sorğular vasitəsi ilə 3-cü tərəflərə məxfi, konfidensial, fərdi, xidməti, o cümlədən maliyyə məlumatlarının göndərilməsi qadağandır;
   10. Qəbul edilməsi gözlənilməyən şübhəli elektron poçtların açılmasından imtina edilməlidir;
   11. Elektron poçt vasitəsi ilə göndərilən qoşma faylların antivirus yoxlamasından keçirilmədən istifadə edilməsi qadağandır.
9. **İnformasiyanın “sosial mühəndislik” yolu ilə əldə edilməsindən qorunma qaydaları**
   1. Əməkdaşların hər hansı kənar sorğuda, naməlum tərəflərin zəngləri ilə verilən sual-cavabda və ya fikir mübadiləsində iştirakı qadağandır;
   2. Şübhəli hər hansı sorğu, anket, məlumat mübadiləsində iştiraka cəlb olunma hallarında və bu halların elektron vasitələrlə aparıldığı hallarda insidentin araşdırılması üçün müvafiq idarə və şöbəyə məlumat verilməlidir;
   3. İstirahət və nahar fasilələrində, xidmətdən kənar vaxtlarda, xüsusən də toplu insan olan yerlərdə xidməti fəaliyyətlə bağlı müzakirələrin aparılması qadağandır;
   4. Qurumun kompüter və şəbəkə haqqındakı texniki, arxitektur, İP və digər parametrlər üzrə məlumatların 3-cü tərəfə ötürülməsi qadağandır;
   5. 3-cü şəxslər tərəfindən göndərilmiş hər hansı texniki tapşırığın razılaşdırılmamış icrası qadağandır;
   6. 3-cü tərəflərin hər hansı məlumat barədə sorğusu, yalnız 3-cü tərəfin kimliyi müəyyənləşdirildikdən və bu məlumatın hansı məqsədlə istifadə olunacağı dəqiqləşdirildikdən sonra cavablandırılmalıdır;
   7. Əcnəbi və ya vətəndaşlığı olmayan şəxslərin fəaliyyət istiqamətinə uyğun olmayan hallar üçün əməkdaşlarla xüsusi münasibəti, əlaqələr qurmaq istəməsi kimi hallar şübhəli hal kimi qiymətləndirilməli və bu barədə müvafiq struktur bölmə məlumatlandırılmalıdır.
10. **Sosial şəbəkə platformalarından təhlükəsiz istifadə qaydaları**
    1. Əməkdaşların sosial şəbəkə platformalarından (Qeyd: bu əlavə quruma görə dəyişə bilər - fəaliyyət (iş, xidmət və s.) yeri (qurumu) bilinməklə) istifadəsi qadağandır;
    2. Yalnız icazə verilən əməkdaşlara xüsusi təyinatlı xidməti tapşırıqları həyata keçirmək məqsədi ilə sosial şəbəkədən istifadəyə şərait yaradılmalıdır;
    3. Fərdi məlumatların, xüsusilə də şəxsiyyəti müəyyən etməyə imkan verən sənədlərdə, əmək haqqı kartında və digər bu kimi sənədlərdə olan məlumatların sosial şəbəkə platformalarında paylaşılması yolverilməzdir;
    4. Səlahiyyəti olmadan qurumun adından danışmaq, utancverici məlumat paylaşmaq, xidməti geyimlə və ya xidmət yerində şəkil çəkdirmək və bu məlumatların yayılmasına yol vermək qadağandır;
    5. Sosial şəbəkə platformalarında qeydiyyat zamanı xidməti məlumatların (telefon, e-poçt ünvanı, ünvan və s.) istifadəsi qadağandır;
    6. Dostluq dəvətləri göndərən naməlum şəxslərin kimliyinə əmin olmadan onların dostluq təklifi, şübhəli məqam kimi qiymətləndirilməlidir;
    7. Sosial şəbəkə sorğularında (“quizz”, xasiyyətin və şəxsi keyfiyyətlərin müəyyən edilməsi ilə bağlı sorğular, “iq” testlər və s.) iştirak etmək qadağandır.
11. **Ağıllı mobil qurğulardan təhlükəsiz istifadə qaydaları**
    1. Əməkdaşların xüsusi rejimli mühafizə zonalarında, istifadəsinə məhdudiyyət tətbiq edilən digər yerlərdə ağıllı telefonlardan istifadə etməsi qadağandır;
    2. Yalnız rəsmi siyahı üzrə müvafiq əməkdaşlara xidməti zərurətlə bağlı təhlükəsizlik tədbirləri (kibergigiyena) gözlənilməklə müəyyən edilmiş ərazilərdə ağıllı telefonlardan istifadə etmək icazəsi verilə bilər;
    3. İstifadəsinə icazə verilən mobil telefon, ağıllı saat və digər avadanlıqlarda “GPS” funksiyası daima sönülü olmalıdır;
    4. Ağıllı mobil qurğularda istifadə edilən bütün proqram tətbiqlərinin (aplikasiya) imtiyaz səviyyələrinə daima nəzarət olunmalıdır;
    5. İstifadə olunan proqram tətbiqlərinin sayı minimum saxlanılmalı, zəruri olmayan tətbiqlər silinməlidir;
    6. Ağıllı mobil qurğular antivirus proqram təminatı ilə təmin olunmalıdır;
    7. Ağıllı mobil qurğuların xidməti şəbəkəyə qoşulması yalnız xüsusi razılıq ilə qeydiyyatı aparılmaqla həyata keçirilə bilər;
    8. Ağıllı mobil qurğulara, xüsusilə xidmət yerlərində və iş saatlarında tanınmayan şəxslər tərəfindən edilən zənglərə cavab verilməsi məqsədəuyğun deyil;
    9. Ağıllı mobil qurğularda xidməti zərurət xaricində video zənglərin qəbul edilməsi qadağandır.
12. **Şifrə təhlükəsizliyi qaydaları:**
    1. Təhkim olunan kompüter, telefon, planşet, noutbuk və ya fərdi kompüterlər unikal şifrələrlə təmin olunmalıdır;
    2. Hər hansı bir kompüterin bir neçə istifadəçisi olarsa hər bir istifadəçiyə ayrı-ayrılıqda hesab və fərdi şifrələr təyin edilməlidir;
    3. Bütün kompüterlər, hesablar (*“login”*) və ya hər hansı informasiya sistemləri təhlükəsiz, təxmin edilməsi mümkün olmayan, “dayanıqlı şifrələr” ilə təmin edilməlidir;
    4. Dövlət internet şəbəkəsində, təhkim olunmuş kompüterlərdə və ya istifadə olunan hər hansı hesab və informasiya sistemində susmaya görə (“default”) olan şifrələrin istifadəsi qəti qadağandır;
    5. Şifrələrin təyini zamanı ad, soyad, ata adı, doğum tarixi, avtomobil seriyası və ya nömrəsi, telefon nömrəsi və s. kimi ictimai məlum məlumatlardan, onların qısaldılmalarından istifadə yolverilməzdir;
    6. Şifrələrin təyini zamanı təkrarlanan hərf, simvol, rəqəmlərdən istifadə etmək yolverilməzdir;
    7. Funksional olaraq mümkün olan bütün hesab və sistemlərdə ikili autentifikasiyadan istifadə olunmalıdır.
13. **İnformasiya daşıyıcılarından istifadə qaydaları**
    1. Bütün informasiya daşıyıcıları[[5]](#footnote-6) şəxsə təhkim olunaraq onun şəxsi inventar kartında qeydiyyata alınmalıdır;
    2. İstənilən məxfi məlumat daşıyıcısı (elektron və ya kağız) yalnız xüsusi bağlı vasitələrdə və ya seyflərdə saxlanılmalıdır;
    3. İşdən azad olunan və ya xidmət sahəsini dəyişən əməkdaş bu informasiya daşıyıcısını təhvil verməlidir19;
    4. Bütün informasiya daşıyıcıları markirovka olunmalı və aidiyyəti üzrə istifadə olunmalıdır;
    5. Xarici (daşınan) yaddaş qurğularının şifrlənmədən (“encrypt”) istifadə edilməsi qadağandır;
    6. Sərgilərdən və bu bənzər digər tədbirlərdən götürülmüş, qonaq qismində müəyyən şirkət təmsilçiləri tərəfindən hədiyyə edilmiş və ya təsadüfən tapılmış yaddaş daşıyıcılarını xidməti kompüterlərə taxmaq və xidməti məqsədlər üçün istifadə etmək qadağandır[[6]](#footnote-7);
    7. Kompüterlərdəki məlumatların “ənənəvi yollarla”[[7]](#footnote-8) (format və s.) silinmədiyini nəzərə alaraq, vəzifə dəyişikliyi və ya xidməti kompüterin yenilənməsi kimi hallarda, köhnə kompüterlərin təhvil verilməsi, digər əməkdaşlara təhkim edilməsi zamanı kompüterdə işlənilən öncəki məlumatların, məlumata giriş icazəsi baxımından daha aşağı səlahiyyətli əməkdaşın əlinə keçməməsi üçün kompüterdəki məlumatlar xüsusi məhevtmə (silinmə) standartına (Gutmann, The DoD 5220.22-M, NAVSO P5239-26, PRNG və s.) uyğun təmizlənməli, imtiyazlar azaldılmalı, internet çıxış qeydiyyatı yenilənməli və yalnız bundan sonra təhvil verilməli, digər əməkdaşa təhkim edilməlidir;
    8. Kağız informasiya daşıyıcıları aiddiyyəti şəxslərin istifadəsi üzrə kargüzarlıq qaydalarına uyğun qeydiyyata alınmalı, mühafizə edilməlidir;
    9. İstifadəsiz kağız informasiya daşıyıcıları xüsusi qaydalar və qurğularla (şreder və s.) məhv edilməlidir.
14. **Buraxılış üzrə təhlükəsizlik qaydaları**
    1. Bütün ərazilərə giriş xidmət sahəsinə və səlahiyyət bölgüsünə görə seqmentləşdirilməli və buna nəzarət xüsusi buraxılış reqlamenti ilə həyata keçirilməlidir;
    2. Buraxılış tanınma vasitələrinin (vəsiqə, buraxılış kartı, bədc, döş nişanı və s.) xidmət sahələrinin icazə verilən əraziləri üzrə uyğunlaşdırılması və ya bölünməsi təmin olunmalıdır;
    3. Səlahiyyəti olmayan şəxslərin buraxılışı məhdudlaşdırılmış xidmət sahələrinə keçməsinə icazə verilməməlidir;
    4. Xidmət sahəsinə buraxılışı olmayan əməkdaşın həmin ərazidə icazəsiz fəaliyyəti qadağandır;
    5. Xidmət sahələrinə buraxılış tanınma vasitəsiləri ilə (vəsiqə, buraxılış kartı, bədc, döş nişanı və s.) həyata keçirilməlidir.
15. **Ezamiyyət, məzuniyyət və işə xitam zamanı informasiya təhlükəsizliyi qaydaları**
    1. Ezamiyyət zamanı informasiya təhlükəsizliyinə daha çox risk yaradan aeroport, kafe, otel və s. ictimai “Wi-Fi” olan ərazilərdə xidməti istifadə üçün ayrılmış kompüter, smartfon, planşet tipli avadanlıqlardan yalnız zərurət yarandığı təqdirdə, təhlükəsizlik tələbləri (kibergigiyena) gözlənilməklə istifadə edilməlidir;
    2. Ezamiyyət, məsafədən (“online”) iş zamanı internetdən istifadə yalnız təhlükəsizliyi təmin edilən, xüsusi şifrli kanal yaradan, qurum tərəfindən istifadəsinə icazə verilmiş “VPN xidməti” vasitəsi ilə həyata keçirilməlidir;
    3. Xidməti istifadədə olan avadanlıqların oğurlanmaması üçün mühafizəyə xüsusi diqqət göstərilməlidir;
    4. Avadanlıqlardan ictimai yerlərdə istifadə zamanı ekranının arxadan izlənməməsi üçün səy göstərilməlidir;
    5. Xarici səfərlərə aparılan informasiya daşıyıcıları daha ciddi və dayanıqlı şifrələr ilə qorunmalıdır;
    6. İnternetdən istifadə zamanı avtorizasiya (qeydiyyat, qaydaların qəbul edilməsi və s. məqsədlərlə) üçün hər hansı bir səhifəyə yönləndirilmə varsa bu, avadanlığın izlənməsinə və komprementasiyasına yol açacağından, belə internetdən istifadədən imtina edilməlidir;
    7. Ezamiyyət zamanı internet klublardan və ya otelin kompüterlərindən xidməti məqsədlər üçün (e-mail ünvanının yoxlanılması, hansısa sənədin hazırlanması və s.) istifadə edilməsi qadağandır;
    8. Zərurət olmadığı təqdirdə xidməti avadanlıqların ezamiyyətə aparılması qadağandır;
    9. İnsan resurslarının idarəetməsinə səlahiyyətli struktur bölmə işinə xitam verilməsi, eləcə də iş yerinin dəyişdirilməsi planlaşdırılan əməkdaşın səlahiyyətlərinin bitmə müddəti barədə Təhlükəsizlik və İT üzrə müvafiq struktur bölməni həmin müddətin bitməsinə ən geçi 2 iş günü qalmış məlumatlandırmalıdır;
    10. İşinə xitam verilən əməkdaşın informasiya sistemlərinə, portallarına, elektron poçt xidmətinə giriş və bu kimi digər imtiyazları dərhal dayandırılmalı, şəbəkəyə giriş imkanları və VPN qoşulmaları (əgər varsa) kəsilməlidir. İş yeri dəyişdirilən əməkdaşın informasiya sistemlərinə, portallarına giriş imtiyazlarına, VPN qoşulma imkanlarına (əgər varsa) dərhal yenidən baxılmalıdır.
16. **Texniki təhlükəsizlik qaydaları**
    1. Bütün texniki avadanlıqlar birkalanmalı (nömrələnməli) və dəqiq inventarizasiya olunmalıdır;
    2. Bütün informasiya sistemlərinin arxitektur dizaynı və texniki sənədləri hazırlanmalı və hər bir sistem üzrə cavabdeh olan müvafiq şəxslər tərəfindən qorunmalıdır;
    3. Bütün kritik sistemlərin dayanıqlı alternativi olmalı, eyni zamanda məlumatlarının mütəmadi olaraq təhlükəsiz formada ehtiyat nüsxəsi çıxarılıb qorunmalıdır, yararlığı plan üzrə sınaqdan keçirilməlidir;
    4. İstifadəyə verilmiş informasiya sisteminin dayanıqlı və fasiləsiz fəaliyyətinə həmin sistem təhkim edilmiş əməkdaş, habelə müvafiq sistemə 24/7 nəzarət üçün ayrılmış növbətçi məsuliyyət daşıyır;
    5. İş vaxtı bitdikdən sonra tərk edilən xidməti otaqda 24/7 fəaliyyəti nəzərdə tutulmayan bütün avadanlıqlar (kompüterlər, printerlər, doldurucular, digər ofis periferiya avadanlıqları və s.) söndürülməlidir.
17. **Yekun müddəalar**
    1. İnformasiya sızmasının qarşısını almaq üçün şəxsi kompüter, mobil telefon və şəxsi istifadə üçün nəzərdə tutulan digər avadanlıqlarda da bu Təlimatda göstərilən tələblərə riayət etməyə səy göstərilməlidir;
    2. Hər hansı dövlət qurumundan informasiya sızıntısı ilə bağlı hər hansı informasiya resursunda, xəbər portallarında və ya sosial şəbəkələrdə paylaşılan məlumatlar xidməti kompüterə birbaşa endirilməməli (adətən belə məlumatlar yoluxdurulmuş olur) və dərhal müvafiq şöbəyə insidentlə bağlı xəbər verilməlidir. Belə informasiyanı yalnız müvafiq stukrutur bölmə həmin məlumatın yoluxdurulmuş olmadığını təsdiq etdikdən sonra endirmək olar;
    3. Təlimatın icra edilməməsi hallarına görə hər bir əməkdaş birbaşa məsuliyyət daşıyır.

1. Bütün informasiya daşıyıcıları qurumun müvafiq struktur bölməsi tərəfindən təmin edilməli və təhkim olunan şəxsin inventar kartında qeydiyyata alınmalıdır. [↑](#footnote-ref-2)
2. Yanlışlıqla klik edilən keçid (URL) və ya kompüterə endirilən zərərverici proqram şəbəkə elementlərinə müdaxilə və ya informasiya oğurluğu üçün kompüterin hakerlər tərəfindən arxa qapı (backdoor) olaraq istifadə edilməsinə imkan yarada bilər. [↑](#footnote-ref-3)
3. Online-offline oyunlar, xüsusən də qumar, idman mərc və “18+” kontentə malik informasiya resurslarından istifadə etmək 95% hallarda kompüterləri zərərvericilərə yoluxduraraq sistemi haker hücumu üçün açıq hala gətirir. [↑](#footnote-ref-4)
4. Fişinq hücumları, şübhəli e-poçt məktubları və popup-lar - fişinq hücumlarında haker adətən özünü əməkdaş kimi təqdim edir və hər hansı bir əməliyyatı görmək üçün şəxsi tələ qurulan veb səhifəyə yönləndirməyə çalışır; [↑](#footnote-ref-5)
5. İnformasiya daşıyıcıları ona yazılan məlumatların zamanla silinməsinə, format olunmasına baxmayaraq, istifadə müddətində ona yazılan bütün xidməti və şəxsi məlumatlar onun daxili yaddaşında qorunur və bu məlumatlar bərpa oluna bilinəndir. Bu baxımdan informasiya daşıyıcılarını ikinci şəxslərə müvəqqəti istifadə üçün və ya birdəfəlik verilməsi zamanı həmin informasiya daşıyıcısında bugünə qədər daşınılan bütün məlumatların da ikinci şəxslərə ötürülməsinin fəsadları dərk edilməlidir. [↑](#footnote-ref-6)
6. Hədiyyə və ya təsadüfən tapılmış yaddaş daşıyıcılarında zərərli, gizlədilmiş agent proqramlarının quraşdırılma hallarındakı statistik artımları nəzərə alaraq belə qurğuların kompüterlərə taxılması və ya xidməti istifadəsi yolverilməzdir. [↑](#footnote-ref-7)
7. Ənənəvi qaydada (delete, shift+delete, format və s.) məlumatların məhv olunması onların tamamilə məhvinə gətirib çıxarmır. İstənilən yaddaş daşıyıcısından (Kompüter, ağıllı telefon, HDD, SSD, Flash yaddaş və s.) ənənəvi yolla silinmiş məlumatları bərpa etmək mümkündür. [↑](#footnote-ref-8)