AZƏRBAYCAN TURİZM VƏ MENECMENT UNİVERSİTETİNDƏ MƏLUMATLARIN İDARƏOLUNMASI ÜZRƏ TƏLİMAT

I Ümumi müddəalar

Azərbaycan Turizm və Menecment Universitetində İKT məlumatlarının idarə olunması və informasiya təhlükəsizliyinin qorunması, Azərbaycan Respublikasi İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında qanuna əsasən formalaşdırılmışdır.

II Məlumatların idarəolunması üzrə planlaşdırma

2.1 Data yaratmağa (toplamağa) başlamazdan əvvəl məlumatları idarə etmək üçün nəzərə alınmalı qərarlar var ki, bunlara formal və ya yarı-formal məlumat planlaması (bir çox layihələrdə məlumatların idarə edilməsi planlarını təqdim edilməli), aparat və proqram təminatı seçimi və intellektual mülkiyyət hüquqlarına aid məsələlər daxildir.

2.2 Başlanğıcda qəbul edilən qərarlar (və ya mümkün qədər tez) gələcəkdə məlumatlarınızı necə əldə etməyinizə, istifadə etməyinizə və saxlamağınıza təsir edəcək.

2.3 Ən yaxşı başlanğıc nöqtəsi odur ki, məlumatların idarə olunması planının yaradılması;

2.4 Məlumatların idarə olunması üçün kifayət qədər texnoloji resurslar vardır (məs., saxlama sahəsi, İT dəstək)

2.5 Məlumatlar etibarlıdır və sənədləşmədə səhvlər yoxdur

2.6 Əldə olunan, yaradılan məlumatlar ani zərər və ya itkilərdən qorunur və hüquqi və etik tələblərə cavab verir

2.7 Hər kəs və ya yuxarı menecerlər istərsə, yekunlaşdırılmış məlumatları açıq şəkildə paylaşa bilər.

2.8 Məlumatlar yaxın, orta və uzaq gələcəkdə əlçatan və başa düşülən olur.

III Formatın müəyyən olunması

3.1 Məlumatları saxlamaq üçün istifadə edilən fayl formatlarını nəzərdən keçirmək zəruridir. Bəzi hallarda, bu istifadə edilən proqram və ya cari layihə tərəfindən müəyyən olunur. Digər hallarda bir neçə variant arasında seçim etmək lazım olur.

Aşağıda qeyd olunanların nəzərə alınması zəruridir:

3.1.1 Gələcəkdə həmkarlar ilə bölüşülməsi asan formatda olan məlumat ;

3.1.2 Yeni formatlardan və ya xüsusi proqramdan asılı olaraq köhnəlmə riski olan formatlar;

3.1.3 Gələcəkdə məlumatları açmağa və oxumağa imkan verən formatlar;

3.1.4 Bəzi hallarda, məlumatların toplanması və təhlili üçün bir formatdan istifadə etmək və layihəniz başa çatdıqdan sonra arxivləşdirmək üçün məlumatlarınızı digər formata çevirmək daha məqsədəuyğundur.

3.2. Məlumatların saxlanılması üçün tövsiyə olunan formatlar:

Mətn məlumatları: DOCX, RTF, TXT, PDF / A (Arxiv PDF)

Cədvəl məlumatları (elektron tablolar daxil olmaqla): XLSX, CSV

Təqdimat məlumatları: PPTX

Verilənlər bazası: XML, CSV

Şəkillər: TIFF, PNG, JPEG (qeyd: JPEG yenidən saxladığınız zaman məlumatları itirən formatdır, yalnız görüntü keyfiyyətinə dair tələbkarlıq etməsəniz onu istifadə edin)

Audio: FLAC, WAV, MP3

IV Data / faylların təşkili və strukturu

4.1 Data faylların və qovluqların məntiqi və ardıcıl şəkildə təşkil edilməsi və adlandırılması, əməkdaşlara və başqalarına onları daha asan tapmaq və istifadə etmək imkanı verir. Bir layihənin başlanğıcında məlumatları necə adlandırmasını və təşkil edilməsi barədə düşünülməli;

4.2 Data fayllarını diqqətlə təşkil etmək vaxta qənaət edir, hər bir əməkdaşa ehtiyac olduqda lazım olan datanı tapmağa kömək etməklə təkrarlanma və ya səhvlərin qarşısını alır.

V Faylları və qovluqları adlandırma

5.1 Məlumatları ardıcıl, məntiqli və gözlənilən şəkildə adlandırmaqla bir-birinə bənzər məlumatları asanlıqla fərqləndirmək olar. Bu zaman məlumatların saxlanması və axtarışı prosesi də asanlaşır;

5.2 Uğurlu təcrübə bütün məlumatların (fayllar, məlumatlar, sənədlər və ya qeydlər) müəyyən və izlənəbilən olması.

VI Datanın etibarlı saxlanılması

6.1 Təhlükəsizlik -məlumatların təsnifatından asılı olmayaraq onların təhlükəsizliyi təmin olunmalı, məlumatlara çıxış nəzarətdə olmalı və onları zədələnməkdən qorunmalı;

6.2 Müəyyənləşdirilməli olan suallar:

- 6.2.1 Həm elektron, həm də fiziki təhlükəsizlik.
- 6.2.2 Təsadüfi və ya qəsdən mümkün zərərin və ya məlumatın dəyişdirilməsinin qarşısının alınması
- 6.2.3 Məlumatların oğurlanması riski.
- 6.2.4 Kimə və hansı məlumatlara çıxış olmalı
- 6.2.5 Məlumat ehtiyatlarına uyğun giriş nəzarəti - məlumatların ətrafında sərhədlərin yaradılması, kimin çıxış edə biləcəyini və əldə edə bilməyəcəyini;
- 6.2.6 Məxfiliyin qorunması və qanunvericiliyin tələblərinə uyğunluq.
- 6.2.7 Qısa, orta və uzun müddətli məlumatları saxlamaq üçün hansı qurğular istifadə olunur.
- 6.2.8 Saxlama cihazlarının, xüsusilə mobil cihazların istifadəsi və təhlükəsizliyi, məs. xarici sərt disk və noutbuklar,müvafiq şifrələmə istifadəsi.
- 6.2.9 Sənədlər həssaslıq səviyyəsinə görə hansı kateqoriyaya aid edilməlidir (müvafiq kateqoriya sənəddə öz əksini tapmalıdır)

6.3 Məlumatların saxlanılması - məlumatları saxlamaq üçün kompüterdə bunun üçün ayrılmış My_Files qovluğu istifadə olunmalı;

6.4 Struktur daxilində yaradılmış faylların son versiyaları mütəmadi olaraq öncədən müəyyən olunmuş məsul əməkdaşın informasiya daşıyıcılarında toplanmalı;

6.5 Bu məlumatlar struktur fəaliyyətini, informasiya sistemlərində baş verə biləcək qəza zamanı tam sığortalamalı;

6.6 Mütəmadi olaraq həmin məlumatların xarici sərt disklərə və məsul şəxsin korporativ bulud hesabına köçürülməsi (nüsxələnməsi) həyata keçirilməli;

6.7 Müəyyən olunmuş məsul şəxs haqqında məlumatlar İnformasiya Texnologiyaları şöbəsinə ötürülməli;

6.8 Ehtiyat nüsxələmə - məlumatların elektron formada nüsxələnməsi məlumatlarının idarə edilməsinin vacib bir hissəsidir. “Ehtiyat nüsxələmə” bir və ya daha çox yerdə məlumatlarınızın surətlərini çıxarılması və saxlamalı;

6.9. Ehtiyat nüsxələmə yalnız Universitetə məxsus məlumatlar üçün nəzərdə tutulur və şəxsi məlumatların nüsxələnmə üçün qəbul olunması mümkün deyil. My_Files qovluğuna daxil edildikdən sonra məlumatlarınız (ilkin halda yalnız məsul şəxslər) avtomatik şəkildə ehtiyat olaraq nüsxələnəcək.

VII İctimai simsiz qonaq şəbəkəsindən istifadə üzrə İstifadəçi razılaşması

7.1 İnformasiya təhlükəsizliyi - informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli, təsadüfi və ya qəsdən təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəli olmasıdır;

7.2 İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

7.3 Şəbəkədən istifadə qaydaları - şəbəkədən istifadə etmək üçün aşağıdakı şərtlər gözlənilməlidir:

7.3.1. Azərbaycan Turizm və Menecment Universitetində ("ATMU") simsiz WiFi şəbəkəsi üzərindən internet xidmətinin təmin olunması;

7.3.2. ATMU WiFi xidməti təqdim edərkən və WiFi xidməti əlçatan olmadıqda sizin (və ya hər hansı bir üçüncü tərəf) qarşısında heç bir məsuliyyət daşımaması;

7.3.3. Xəbərdarlıq etmədən və bizim təqdirimizlə WiFi xidmətinə xitam verə bilməsi;

7.3.4. Şəbəkə vasitəsilə vətəndaşların şərəf və ləyaqətini təhqir edən məlumatları yaymaq və ya yayılmasına şərait yaratmamaq;

7.3.5. İT şöbənin icazəsi olmadan kanalların yüklənməsinə səbəb olacaq kanalhəcmli resurlarla işləməməli (real video, real audio, çat və s);

7.3.6. ATMU-da WiFi xidmətindən istifadə tamamilə öz riskiniz üzərində olması və hər hansı bir itkiyə görə heç bir məsuliyyət qəbul edilməməsi;

7.3.7. ATMU-nun WiFi şəbəkəsinin istənilən cihaz və ya qurğu ilə uyğun olacağına zəmanət verilməməsi;

7.3.8. WiFi xidmətindən istifadə etmək və ya daxil olmaq sizin avadanlıq və ya cihazınızın vəziyyəti səbəbindən mümkün olmadıqda, avadanlıq və ya cihazınızın işə yaramaması üçün məsuliyyət daşınmaması;.

7.3.9. ATMU, WiFi şəbəkəsi üzərindən göndərilən məlumatların təhlükəsizliyinə zəmanət verilməməsi və bu məlumatların başqalarına əlçatan ola biləcəyinə dair xəbərdarlıq edilməsi;

7.3.10. ATMU-nun sizin fəaliyyətinizin gizliliyi və təhlükəsizliyi üçün heç bir məsuliyyət daşımaması. İnternetdə kredit kartı məlumatları kimi məxfi informasiyaların ötürülməsi zamanı fərdi təhlükəsizlik "firewall"-dan istifadə edilməsi və lazımi ehtiyat tədbirlərinin alınmasının zəruriliyi. Onlayn təhlükəsizliyə dair daha ətraflı məlumat üçün www.getsafeonline.org ünvanına daxil olaraq internet vasitəsilə məxfi informasiyaların göndərilməsindən yaranan zərərlər üçün ATMU-nun heç bir məsuliyyət daşımaması;.

7.3.11. Cihaz və ya aparatınızı antivirus və zərərli proqramlara qarşı proqram təminatı ilə təmin etmək sizin öhdəliyinizdir. Kafi təhlükəsizlik parametrləri və ya müvafiq proqramı təminatı istifadə etməməyiniz səbəbindən yaranmış zərər və bizim WiFi xidmətindən istifadə edərkən cihazınıza yüklənə biləcək hər hansı bir virus və ya casus proqramı üçün ATMU-nun məsuliyyət daşımaması;

7.3.12. WiFi xidmətindən istifadə etməyinizlə bağlı sizə texniki yardım göstərilməsinin mümkün olmamasının nəzərə alınması;

7.3.13. WiFi xidməti üzərindən çap etməyin mümkün olmamasının;

7.3.14. WiFi şəbəkəmiz üzərindən World Wide Web'ə çıxış təmin olunsa da, telnet, ftp və ya Internet Relay Chat tipli qoşulmaların əlçatan olmamasının nəzərə alınması;

7.3.15. Uyğun olmayan məzmuna girişin minimuma endirilməsi üçün müəyyən veb saytlar filtrasiya proqramı ilə məhdudlaşdırırılır. Buna baxmayaraq, bu proqram təminatının həmişə bu tip məzmuna giriş üçün mane ola bilməməsi və hər hansı bir uyğunsuz saytlar bloklanmadıqda ATMU-nun məsuliyyət daşımaması.