BEYNƏLXALQ STANDART

ISO/IEC 27701

Birinci nəşr
2019-08

Təhlükəsizlik üsulları — Fərdi məlumatların idarə edilməsi ilə bağlı ISO/IEC 27001 və ISO/IEC 27002 standartlarına əlavə — Tələblər və təlimatlar

Mündəricat

Səhifə

Ön Söz

Beynəlxalq Standartlaşdırma Təşkilatı (ISO) və Beynəlxalq Elektrotexnika Komissiyası (IEC) qlobal səviyyədə standartlaşdırma üzrə ixtisaslaşdırılmış sistemi formalaşdırır. ISO-nun və ya IEC-in üzvləri olan milli orqanlar müvafiq təşkilat tərəfindən yaradılmış texniki komitələr vasitəsilə texniki fəaliyyətin xüsusi sahələri ilə məşğul olmaq üçün beynəlxalq standartların hazırlanması prosesində iştirak edir. ISO-nun və IEC-in texniki komitələri qarşılıqlı maraq doğuran sahələrdə əməkdaşlıq edirlər. Bu işdə beynəlxalq təşkilatlar, həmçinin hökumət və qeyri-hökumət təşkilatları da ISO və IEC ilə əməkdaşlıq şərtlərində iştirak edir.

Bu sənədi hazırlamaq üçün istifadə olunan və onun sonrakı saxlanması üçün nəzərdə tutulan prosedurlar ISO/IEC Direktivlərinin 1-ci hissəsində təsvir edilir. Xüsusən, müxtəlif növ sənədlər üçün tələb olunan fərqli təsdiq meyarları qeyd edilməlidir. Bu sənəd ISO/IEC Direktivlərinin 2-ci hissəsinin redaksiya qaydalarına uyğun olaraq tərtib olunub (baxın: www.iso.org/directives).

Bu sənədin bəzi elementlərinin patent hüquqlarının predmeti ola biləcəyi ehtimalına diqqət yetirilir. ISO və IEC bu cür patent hüquqlarının hər hansı birinin və ya hamısının müəyyən edilməsinə görə məsuliyyət daşımır. Sənədin hazırlanması zamanı müəyyən edilmiş hər hansı patent hüquqlarının təfərrüatları "Giriş" bölməsində və/yaxud ISO-nun daxil olmuş patent bəyannamələrinin siyahısında (baxın: www.iso.org/patents) və ya IEC -in daxil olmuş patent bəyannamələrinin siyahısında (baxın: http://patents.iec.ch) təqdim olunacaq.

Bu sənəddə istifadə edilən hər hansı ticarət adı istifadəçilərin rahatlığı üçün verilən informasiyadır və onun dəstəkləndiyini ehtiva etmir.

Standartların könüllü xarakter daşıması, uyğunluğun qiymətləndirilməsi ilə bağlı ISO-nun xüsusi termin və ifadələrinin mənasına dair izahat, eləcə də ISO-nun Ümumdünya Ticarət Təşkilatının (ÜTT) Ticarətə Texniki Maneələr Sazişində əksini tapan prinsiplərə sadiqliyi haqqında məlumat almaq üçün aşağıdakı keçidə daxil ola bilərsiniz: www.iso.org/iso/foreword.html.

Bu sənəd ISO-nun *İnformasiya Texnologiyası* üzrə ISO/IEC JTC 1 saylı Birgə Texniki Komitəsinin *Təhlükəsizlik üsulları* üzrə SC 27 saylı Altkomitəsi tərəfindən hazırlanıb.

Bu sənədlə bağlı hər hansı rəy və ya suallar istifadəçinin milli standartlaşdırma orqanına yönəldilməlidir. Bu orqanların tam siyahısı www.iso.org/members.html səhifəsində təqdim olunur.

Giriş

0.1 Ümumi müddəalar

Demək olar ki, hər bir təşkilat Fərdi Eyniləşdirilə bilən Məlumatları (FEM) emal edir. Bundan əlavə, bir təşkilatın digər təşkilatlarla FEM-in emalı ilə bağlı əməkdaşlıq etməli olduğu hallar artdıqca emal edilən FEM-in miqdarı və növləri də artmaqdadır. FEM-in emalı kontekstində şəxsi həyatın toxunulmazlığının qorunması sosial zərurət, eləcə də bütün dünyada xüsusi qanunvericilikdə və/və ya normativ aktlarda nəzərə alınan mövzudur.

ISO/IEC 27001-də müəyyən edilən İnformasiya Təhlükəsizliyini İdarəetmə Sistemi (İTİS) yeni bir İdarəetmə Sisteminin hazırlanmasına ehtiyac olmadan sektorlar üzrə tələblərin əlavə edilməsinə icazə verəcək formada hazırlanıb. ISO İdarəetmə Sistemi standartları, o cümlədən sektorlar üzrə standartlar ayrıca və ya birgə İdarəetmə Sistemi olaraq icra oluna biləcək formada hazırlanıb.

FEM-in mühafizəsi üzrə tələblər və göstərişlər xüsusən milli qanunvericiliyin və/və ya normativ aktların mövcud olduğu halda təşkilatın kontekstindən asılı olaraq dəyişir. ISO/IEC 27001 bu kontekstin başa düşülməsini və nəzərə alınmasını tələb edir. Bu sənəd aşağıdakılara uyğun strukturlaşdırmanı ehtiva edir:

— ISO/IEC 29100-da müəyyən edilmiş şəxsi həyatın toxunulmazlığı çərçivəsi və prinsipləri

— ISO/IEC 27018;

— ISO/IEC 29151; və

— Aİ-nin Fərdi Məlumatların Mühafizəsinə dair Ümumi Qaydaları.

Lakin bunlar yerli qanunvericiliyi və/və ya normativ aktları nəzərə alaraq şərh edilməli ola bilər.

Bu sənəddən FEM nəzarətçiləri (o cümlədən birgə FEM nəzarətçiləri) və FEM-i emal edən tərəflər (o cümlədən subpodrat müqaviləsi əsasında cəlb olunan FEM emal edən subpodratçılardan istifadə edənlər və FEM-i emal edən tərəflər adından FEM emal edən subpodratçılar) istifadə edə bilər.

Bu sənəddəki tələblərə əməl edən təşkilat FEM-in emalını necə idarə etdiyinə dair yazılı sübutlar hazırlayacaq. Bu cür sübutlar FEM-in emalının qarşılıqlı formada uyğun olduğu biznes tərəfdaşları ilə müqavilələrin bağlanmasına kömək etmək üçün istifadə oluna bilər. O, həmçinin digər maraqlı tərəflərlə münasibətlərə də kömək edə bilər. Bu sənəddən ISO/IEC 27001 ilə birlikdə istifadə edilməsi, istənilərsə, bu sübutun müstəqil şəkildə yoxlanılmasını təmin edə bilər.

Bu sənəd ilk olaraq ISO/IEC 27552 kimi hazırlanıb.

0.2 Digər idarəetmə sistemi standartlarına uyğunluq

Bu sənəd ISO tərəfindən İdarəetmə Sistemi Standartları arasında uzlaşmanı təkmilləşdirmək üçün hazırlanmış çərçivəni tətbiq edir.

Bu sənəd təşkilata özünün Fərdi Məlumatların İdarə edilməsi Sistemini (FMİS) digər İdarəetmə Sistemi standartlarının tələbləri ilə uyğunlaşdırmağa və ya inteqrasiya etməyə imkan verir.

Təhlükəsizlik üsulları — Fərdi məlumatların idarə edilməsi üçün ISO/IEC 27001 və ISO/IEC 27002 standartlarına əlavə — Tələblər və göstərişlər

1 Tətbiq sahəsi

Bu sənəd təşkilatın konteksti çərçivəsində şəxsi həyatın toxunulmazlığının idarə edilməsi üçün ISO/IEC 27001 və ISO/IEC 27002 standartlarına əlavə formasında Fərdi Məlumatların İdarə edilməsi Sisteminin (FMİS) yaradılması, icrası, texniki xidmətlə təmin edilməsi və davamlı təkmilləşdirilməsi üçün tələbləri müəyyənləşdirir və göstərişlər təmin edir.

Bu sənəd FEM-in emalı üzrə öhdəliyi və hesabatlılığı olan FEM nəzarətçiləri və FEM-i emal edən tərəflər üçün FMİS ilə əlaqəli tələbləri müəyyənləşdirir və göstərişlər təmin edir.

Bu sənəd İTİS çərçivəsində FEM-in emalını həyata keçirən FEM nəzarətçiləri və/və ya FEM-i emal edən tərəflər olan bütün təşkilat növləri və ölçüləri üçün, o cümlədən dövlət və özəl şirkətlər, dövlət qurumları və qeyri-kommersiya təşkilatları üçün nəzərdə tutulur.

2 Normativ sənədlərə istinadlar

Mətndə aşağıdakı sənədlərə elə istinad edilir ki, onların məzmununun bir hissəsi və ya hamısı bu sənədin tələblərini təşkil edir. Tarixi göstərilən istinadlar üçün yalnız istinad edilən versiya uyğundur. Tarixi göstərilməyən istinadlar üçün isə istinad edilən sənədin ən son versiyası (o cümlədən ona edilən hər hansı düzəliş) uyğundur.

ISO/IEC 27000, *İnformasiya texnologiyaları — Təhlükəsizlik üsulları — İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri — İcmal və lüğət*

ISO/IEC 27001:2013, *İnformasiya texnologiyaları — Təhlükəsizlik üsulları — İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri — Tələblər*

ISO/IEC 27002:2013, *İnformasiya texnologiyaları — Təhlükəsizlik üsulları — İnformasiya təhlükəsizliyinə nəzarət tədbirləri üçün praktiki qaydalar*

ISO/IEC 29100, *İnformasiya texnologiyaları — Təhlükəsizlik üsulları — Şəxsi həyatın toxunulmazlığı çərçivəsi*

3 Terminlər, tərifləر və ixtisarlar

Bu sənəd çərçivəsində ISO/IEC 27000 və ISO/IEC 29100 standartlarında verilən terminlər və tərifləر və aşağıdakılar tətbiq edilir.

ISO və IEC standartlaşdırmada istifadə ediləcək terminoloji məlumat bazalarını aşağıdakı veb-ünvanlarda saxlayır:

— ISO-nun onlayn axtarış platforması: https://www.iso.org/obp

— IEC Elektropediyası: http://www.electropedia.org/

3.1
Birgə FEM nəzarətçisi
FEM-in emalının məqsədlərini və vasitələrini bir və ya daha artıq digər FEM nəzarətçiləri ilə birgə şəkildə müəyyənləşdirən FEM nəzarətçisi

3.2
fərdi məlumatların idarə edilməsi sistemi
(FMİS)
potensial şəkildə FEM-in emalının təsirinə məruz qalan şəxsi həyatın toxunulmazlığının qorunmasını əhatə edən informasiya təhlükəsizliyinin idarə edilməsi sistemi

4 Ümumi müddəalar

4.1 Bu sənədin strukturu

Bu, ISO/IEC 27001:2013 və ISO/IEC 27002:2013 standartları ilə bağlı sektora aid sənəddir.

Bu sənəd FMİS-ə aid tələbləri əhatə edir. Bu sənədə uyğunluq bu tələblərə və ISO/IEC 27001:2013 standartında olan tələblərə əməl edilməsinə əsaslanır. Bu sənəd ISO/IEC 27001:2013 tələblərini informasiya təhlükəsizliyinə əlavə olaraq, potensial şəkildə FEM-in emalının təsirinə məruz qalan FEM subyektlərinin şəxsi həyatının toxunulmazlığının qorunmasını nəzərə alaraq genişləndirir. Müxtəlif məqamların daha yaxşı başa düşülməsi üçün icra üzrə göstərişlər və tələblərlə bağlı digər məlumatlar sənədə daxil edilib.

Maddə 5 ISO/IEC 27001 standartında FEM nəzarətçisi və ya FEM-i emal edən tərəf kimi çıxış edən təşkilata uyğun olan informasiya təhlükəsizliyi tələbləri ilə bağlı FMİS-ə aid tələbləri və digər məlumatları təqdim edir.

QEYD 1: Maddə 5 bütün müvafiq məsələlərin əhatə olunması məqsədilə FMİS-ə aid tələblərin və ya digər məlumatların olmadığı hallarda belə ISO/IEC 27001:2013-dəki tələbləri ehtiva edən hər bir maddə üçün bir bəndi ehtiva edir.

Maddə 6 ISO/IEC 27002-də FEM nəzarətçisi və ya FEM-i emal edən tərəf kimi çıxış edən təşkilat üçün informasiya təhlükəsizliyinə nəzarət tədbirləri ilə bağlı FMİS-ə aid göstərişləri və digər məlumatları təqdim edir.

QEYD 1: Maddə 6 bütün müvafiq məsələlərin əhatə olunması məqsədilə FEMİS-ə aid göstərişlərin və ya digər məlumatların olmadığı hallarda belə ISO/IEC 27002:2013-dəki məqsədləri və ya nəzarət tədbirlərini ehtiva edən hər bir maddə üçün bir bəndi ehtiva edir.

Maddə 7 FEM nəzarətçiləri üçün ISO/IEC 27002 üzrə əlavə göstərişləri, Maddə 8 isə FEM-i emal edən tərəflər üçün ISO/IEC 27002 üzrə əlavə göstərişləri təqdim edir.

Qoşma A-da FEM nəzarətçisi kimi çıxış edən təşkilat (FEM-i emal edən tərəfə sahib olub-olub-olmamasından və başqa bir FEM nəzarətçisi ilə birgə hərəkət edib-etməməsindən asılı olmayaraq) üçün FMİS-ə aid nəzarət məqsədləri və nəzarət tədbirləri sadalanır.

Qoşma B-də FEM-i emal edən tərəf kimi çıxış edən təşkilat (FEM-in emalı üçün ayrıca FEM-i emal edən tərəfi subpodrat müqaviləsi əsasında cəlb edib-etməməsindən asılı olmayaraq və o cümlədən FEM-in emalını FEM-i emal edən tərəf adından subpodratçılar kimi həyata keçirənlər) üçün FMİS-ə aid nəzarət məqsədləri və nəzarət tədbirləri sadalanır.

Qoşma C ISO/IEC 29100 standartına uyğun strukturlaşdırılmanı ehtiva edir.

Qoşma D bu sənəddəki nəzarət tədbirlərinin Aİ-nin Fərdi Məlumatların Mühafizəsinə dair Ümumi Qaydalarına uyğun şəkildə strukturlaşdırılmasını ehtiva edir.

Qoşma E ISO/IEC 27018 və ISO/IEC 29151 standartlarına uyğun strukturlaşdırılmanı ehtiva edir.

Qoşma F-də FEM emal ediləndə ISO IEC 27001 və ISO/IEC 27002 standartlarının şəxsi həyatın toxunulmazlığına necə şamil edilməsi izah edilir.

4.2 ISO/IEC 27001:2013 tələblərinin tətbiqi

Cədvəl 1-də ISO/IEC 27001 ilə bağlı bu sənəddəki FMİS-ə aid tələblərin yeri təqdim edilir.

Cədvəl 1 — ISO/IEC 27001:2013 standartında nəzarət tədbirlərinin icrası üçün FMİS-ə aid tələblərin və digər məlumatların yeri

ISO/IEC 27001:2013-də maddə	Başlıq	Bu sənədin bəndi	Qeydlər
4	Təşkilati mühit	5.2	Əlavə tələblər
5	Liderlik	5.3	FMİS-ə aid heç bir tələb yoxdur
6	Planlaşdırma	5.4	Əlavə tələblər
7	Dəstək	5.5	FMİS-ə aid heç bir tələb yoxdur
8	Əməliyyat	5.6	FMİS-ə aid heç bir tələb yoxdur
9	Fəaliyyət effektivliyinin qiymətləndirilməsi	5.7	FMİS-ə aid heç bir tələb yoxdur
10	Təkmilləşmə	5.8	FMİS-ə aid heç bir tələb yoxdur

QEYD: "İnformasiya təhlükəsizliyi" anlayışının 5.1 bəndinə əsasən genişləndirilmiş şərhi FMİS-ə aid tələblər olmadıqda belə həmişə tətbiq edilir.

4.3 ISO/IEC 27002:2013 təlimatlarının tətbiqi

Cədvəl 2-də ISO/IEC 27002 ilə bağlı bu sənəddəki FMİS-ə aid göstərişlərin yeri təqdim edilir.

Cədvəl 2 — ISO/IEC 27002:2013-də nəzarət tədbirlərinin icrası üçün FMİS-ə aid göstərişlərin və digər məlumatların yeri

ISO/IEC 27002:2013-də maddələr	Başlıq	Bu sənədin bəndi	Qeydlər
5	İnformasiya təhlükəsizliyi siyasətləri	6.2	Əlavə göstərişlər
6	İnformasiya təhlükəsizliyinin təşkil edilməsi	6.3	Əlavə göstərişlər
7	Kadrların təhlükəsizliyi	6.4	Əlavə göstərişlər
8	Aktivlərin idarə edilməsi	6.5	Əlavə göstərişlər
9	Çıxış imkanına nəzarət	6.6	Əlavə göstərişlər
10	Kriptoqrafiya	6.7	Əlavə göstərişlər
11	Fiziki və ətraf mühit təhlükəsizliyi	6.8	Əlavə göstərişlər
12	Əməliyyatların təhlükəsizliyi	6.9	Əlavə göstərişlər
13	Kommunikasiya təhlükəsizliyi	6.10	Əlavə göstərişlər
14	Sistemlərin əldə edilməsi, tərtibatı və texniki xidmətlə təmin olunması	6.11	Əlavə göstərişlər
15	Təchizatçılarla əlaqələr	6.12	Əlavə göstərişlər
16	İnformasiya təhlükəsizliyi üzrə insidentlərin idarə olunması	6.13	Əlavə göstərişlər
17	İşin davamlılığının idarə edilməsinin informasiya təhlükəsizliyi aspektləri.	6.14	FMİS-ə aid heç bir göstəriş yoxdur
18	Uyğunluq	6.15	Əlavə göstərişlər

QEYD: "İnformasiya təhlükəsizliyi" anlayışının6.1 bəndinə əsasən genişləndirilmiş şərhi FMİS-ə aid göstərişlər olmadığı halda belə tətbiq şamil edilir.

4.4 Müştəri

Təşkilatın rolundan asılı olaraq (baxın: 5.2.1), "müştəri" anlayışı aşağıdakı kimi başa düşülə bilər:

a) FEM nəzarətçisi ilə müqavilə bağlayan təşkilat (məs., FEM nəzarətçisinin müştərisi);

QEYD 1 Bu, təşkilatın birgə nəzarətçi olduğu halda ola bilər.

QEYD 2 Bu sənəddə təşkilatla biznesdən istehlakçıya (B2C) formasında münasibəti olan fərdi şəxs dedikdə "FEM-in subyekti" nəzərdə tutulur.

b) FEM-i emal edən tərəf ilə müqavilə bağlayan FEM nəzarətçisi (məs., FEM-i emal edən tərəfin müştərisi); və ya

c) FEM-in emalı üçün subpodratçı ilə müqavilə bağlayan FEM-i emal edən tərəf (məs., subpodrat müqaviləsi əsasında cəlb olunan FEM emal edən subpodratçının müştərisi).

QEYD 3 Maddə 6-da "müştəri" anlayışından istifadə edildikdə müvafiq müddəalar a), b) və ya c) kontekstlərində münasib ola bilər.

QEYD 4 Maddə 7 və Qoşma A-da "müştəri" anlayışından istifadə edildikdə müvafiq müddəalar a) kontekstində münasibdir.

QEYD 5 Maddə 8 və Qoşma B-də "müştəri" anlayışından istifadə edildikdə müvafiq müddəalar b) və/və ya c) kontekstlərində münasib ola bilər.

5 ISO/IEC 27001 standartının əsasında FMİS-ə aid tələblər

5.1 Ümumi müddəalar

ISO/IEC 27001:2013 standartının "informasiya təhlükəsizliyi"ndən bəhs edən tələbləri potensial şəkildə FEM-in emalının təsir etdiyi şəxsi həyatın toxunulmazlığının qorunmasına tətbiq edilməlidir.

QEYD: Praktikada ISO/IEC 27001:2013-də "informasiya təhlükəsizliyi" anlayışının istifadə olunduğu hallarda onun əvəzinə "informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı" anlayışı nəzərdə tutulur (baxın: Qoşma F).

5.2 Təşkilati mühit

5.2.1 Təşkilatın və onun kontekstinin başa düşülməsi

ISO/IEC 27001:2013 standartının 4.1 bəndinə əlavə tələb aşağıdakı kimidir:

Təşkilat FEM nəzarətçisi (o cümlədən birgə FEM nəzarətçisi) və/və ya FEM-i emal edən tərəf kimi öz rolunu müəyyənləşdirməlidir.

Təşkilat öz kontekstinə uyğun olan və öz FMİS-nin nəzərdə tutulan nəticəsinə (nəticələrinə) nail olmaq bacarığına təsir edən xarici və daxili amilləri müəyyənləşdirməlidir. Məsələn, bunlara aşağıdakılar daxil ola bilər:

— şəxsi həyatın toxunulmazlığı üzrə tətbiq olunan qanunvericilik;

— tətbiq olunan hüquqi sənədlər;

— müvafiq məhkəmə qərarları;

— müvafiq təşkilati kontekst, idarəçilik, siyasətlər və prosedurlar;

— tətbiq olunan inzibati qərarlar;

— tətbiq olunan müqavilə əsaslı tələblər.

Təşkilat hər iki rolda çıxış etdikdə (məs., FEM nəzarətçisi və FEM-i emal edən tərəf), hər biri fərqli nəzarət elementinə malik olan ayrıca rollar müəyyənləşdirilməlidir.

QEYD: Təşkilatın vəzifəsi FEM-in emalının hər bir nümunəsi üçün fərqli ola bilər, çünki o, məlumatların emalının məqsədlərini və vasitələrini kimin müəyyənləşdirməsindən asılı olur.

5.2.2 Maraqlı tərəflərin ehtiyaclarının və gözləntilərinin başa düşülməsi

ISO/IEC 27001:2013 standartının 4.2 bəndinə əlavə tələb aşağıdakı kimidir:

Təşkilat FEM-in emalı ilə əlaqəli maraqları və ya məsuliyyətləri olan tərəfləri, o cümlədən FEM subyektlərini öz maraqlı tərəflərinə (baxın: ISO/IEC 27001:2013, 4.2) daxil etməlidir.

QEYD 1 Digər maraqlı tərəflərə müştərilər (baxın: 4.4), nəzarət orqanları, digər FEM nəzarətçiləri, FEM-i emal edən tərəflər və onların subpodratçıları daxil ola bilər.

QEYD 2: FEM-in emalı ilə bağlı tələblər hüquqi və normativ tələblər, müqavilə əsaslı öhdəliklər və müstəqil olaraq təyin edilmiş təşkilati məqsədlər əsasında müəyyənləşdirilə bilər. ISO/IEC 29100-da təyin edilmiş şəxsi həyatın toxunulmazlığı prinsipləri FEM-in emalı ilə bağlı göstərişləri müəyyən edir.

QEYD 3: Təşkilatın öhdəliklərinə uyğunluğu nümayiş etdirən element kimi bəzi maraqlı tərəflər təşkilatın bu sənəddə müəyyən edilən İdarəetmə Sistemi kimi xüsusi standartlara və/və ya hər hansı bir sıra müvafiq tələblərə əməl etməsini gözləyə bilərlər. Bu tərəflər bu standartlara uyğunluğa dair müstəqil auditin keçirilməsini tələb edə bilərlər.

5.2.3 İnformasiya təhlükəsizliyinin idarə edilməsi sisteminin tətbiq sahəsinin müəyyən edilməsi

ISO/IEC 27001:2013 standartının 4.3 bəndinə əlavə tələb aşağıdakı kimidir:

FMİS-nin tətbiq sahəsini müəyyənləşdirərkən təşkilat FEM-in emalını daxil etməlidir.

QEYD: FMİS-nin tətbiq sahəsinin müəyyən edilməsi "informasiya təhlükəsizliyi" anlayışının5.1 bəndinə əsasən genişləndirilmiş şərhinə görə informasiya təhlükəsizliyinin idarə edilməsi sisteminin tətbiq sahəsinə yenidən baxılmasını tələb edə bilər.

5.2.4 İnformasiya təhlükəsizliyinin idarə edilməsi sistemi

ISO/IEC 27001:2013 standartının 4.4 bəndinə əlavə tələb aşağıdakı kimidir:

Təşkilat ISO/IEC 27001:2013 standartının Maddə 5-dəki tələblərə görə genişləndirilən Maddə 4-dən Maddə 10-dakı tələblərə uyğun olaraq, FMİS yaratmalı, icra etməli, texniki xidmətlə təmin etməli və onu davamlı şəkildə təkmilləşdirməlidir.

5.3 Liderlik

5.3.1 Liderlik və öhdəliklərə sadiqlik

ISO/IEC 27001:2013 standartının 5.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.3.2 Siyasət

ISO/IEC 27001:2013 standartının 5.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.3.3 Təşkilati vəzifələr, məsuliyyətlər və səlahiyyətlər

ISO/IEC 27001:2013 standartının 5.3 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.4 Planlaşdırma

5.4.1 Risklər və imkanlarla bağlı görülməli tədbirlər

5.4.1.1 Ümumi müddəalar

ISO/IEC 27001:2013 standartının 6.1.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.4.1.2 İnformasiya təhlükəsizliyi üzrə risklərin qiymətləndirilməsi

ISO/IEC 27001:2013 standartının 6.1.2 bəndində göstərilən tələblər aşağıdakı təkmilləşdirmələrlə tətbiq olunur:

ISO/IEC 27001:2013, 6.1.2 c) 1) aşağıdakı kimi təkmilləşdirilir:

Təşkilat FMİS-in tətbiq sahəsində məxfiliyin, toxunulmazlığın və əlçatanlığın itməsi ilə əlaqəli riskləri müəyyənləşdirmək üçün informasiya təhlükəsizliyinə dair risklərin qiymətləndirilməsi prosesini tətbiq etməlidir.

Təşkilat FMİS-in tətbiq sahəsində FEM-in emalı ilə əlaqəli riskləri müəyyənləşdirmək üçün şəxsi həyatın toxunulmazlığına dair risklərin qiymətləndirilməsi prosesini həyata keçirməlidir.

Təşkilat bütün risklərin qiymətləndirilməsi proseslərində informasiya təhlükəsizliyi ilə FEM-in mühafizəsi arasındakı əlaqənin müvafiq şəkildə idarə edilməsini təmin etməlidir.

QEYD: Təşkilat ya kompleks informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığına dair risklərin qiymətləndirilməsi prosesini, ya da informasiya təhlükəsizliyi və FEM-in emalı ilə əlaqəli risklər üçün iki ayrıca proses tətbiq edə bilər.

ISO/IEC 27001:2013, 6.1.2 d) 1) aşağıdakı kimi təkmilləşdirilir:

Təşkilat yuxarıda təkmilləşdirilmiş ISO/IEC 27001:2013, 6.1.2 c) bəndində müəyyən edilən risklər reallaşacağı halda həm təşkilat, həm də FEM subyektləri üçün ortaya çıxa biləcək potensial nəticələri qiymətləndirməlidir.

5.4.1.3 İnformasiya təhlükəsizliyi üzrə risklərin aradan qaldırılması

ISO/IEC 27001:2013 standartının 6.1.3 bəndində göstərilən tələblər aşağıdakı əlavələrlə tətbiq olunur:

ISO/IEC 27001:2013, 6.1.3 c) aşağıdakı kimi təkmilləşdirilir:

ISO/IEC 27001:2013 6.1.3 b) bəndində müəyyənləşdirilən nəzarət tədbirləri heç bir zəruri nəzarət tədbirlərinin istisna edilmədiyini təsdiqləmək üçün Qoşma A və/və ya Qoşma B-dəki və ISO/IEC 27001:2013 standartında Qoşma A-dakı nəzarət tədbirləri ilə müqayisə edilməlidir.

Risklərin aradan qaldırılması üçün ISO/IEC 27001:2013 standartının Qoşma A hissəsində nəzarət məqsədlərinin və nəzarət tədbirlərinin tətbiq olunma qabiliyyətini qiymətləndirərkən nəzarət məqsədləri və nəzarət tədbirləri həm informasiya təhlükəsizliyinə, həm də FEM-in emalına, o cümlədən FEM subyektlərinə yönəlmiş risklər kontekstində nəzərə alınmalıdır.

ISO/IEC 27001:2013, 6.1.3 d) aşağıdakı kimi təkmilləşdirilir:

Aşağıdakıları ehtiva edən Tətbiq Bəyanatı hazırlamaq:

— vacib nəzarət tədbirləri [baxın: ISO/IEC 27001:2013, 6.1.3 b) və c)];

— onların daxil edilməsi üçün əsaslandırma;

— vacib nəzarət tədbirlərinin icra edilib-edilməməsi; və

— təşkilatın öz rolunu müəyyənləşdirməsinə əsasən Qoşma A və/və ya Qoşma B və ISO/IEC 27001:2013 standartının Qoşma A hissəsindəki hər hansı nəzarət tədbirinin istisna edilməsi üzrə əsaslandırma (baxın: 5.2.1).

Qoşmalarda sadalanan nəzarət məqsədlərinin və nəzarət tədbirlərinin hamısının FMİS-in icrasına daxil edilməsinə ehtiyac yoxdur. İstisnaya dair əsaslandırmaya nəzarət tədbirlərinin risklərin qiymətləndirilməsinə görə

zəruri hesab edilmədiyi və qanunvericilik və/və ya normativ aktlar, o cümlədən FEM-in subyektinə şamil edilən normativ aktların tələb etmədiyi (və ya istisnalara məruz qaldığı) hallar daxil ola bilər.

5.4.2 İnformasiya təhlükəsizliyi məqsədləri və onlara nail olmaq üçün planlaşdırma

ISO/IEC 27001:2013 standartının 6.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5 Dəstək

5.5.1 Resurslar

ISO/IEC 27001:2013 standartının 7.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.2 Sərişte

ISO/IEC 27001:2013 standartının 7.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.3 Məlumatlılıq

ISO/IEC 27001:2013 standartının 7.3 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.4 Kommunikasiya

ISO/IEC 27001:2013 standartının 7.4 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.5 Sənədləşdirilmiş informasiya

5.5.5.1 Ümumi müddəalar

ISO/IEC 27001:2013 standartının 7.5.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.5.2 Sənədləşdirilmiş informasiyaların yaradılması və yenilənməsi

ISO/IEC 27001:2013 standartının 7.5.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.5.5.3 Sənədləşdirilmiş informasiyaya nəzarət

ISO/IEC 27001:2013 standartının 7.5.3 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.6 Əməliyyat

5.6.1 Əməliyyatın planlaşdırılması və ona nəzarət

ISO/IEC 27001:2013 standartının 8.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.6.2 İnformasiya təhlükəsizliyi üzrə risklərin qiymətləndirilməsi

ISO/IEC 27001:2013 standartının 8.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.6.3 İnformasiya təhlükəsizliyi üzrə risklərin aradan qaldırılması

ISO/IEC 27001:2013 standartının 8.3 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.7 Fəaliyyət effektivliyinin qiymətləndirilməsi

5.7.1 Monitorinq, ölçmə, təhlil və qiymətləndirmə

ISO/IEC 27001:2013 standartının 9.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.7.2 Daxili audit

ISO/IEC 27001:2013 standartının 9.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.7.3 Rəhbərlik tərəfindən baxış

ISO/IEC 27001:2013 standartının 9.3 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.8 Təkmilləşmə

5.8.1 Uyğunsuzluq və təshihedici tədbirlər

ISO/IEC 27001:2013 standartının 10.1 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

5.8.2 Davamlı təkmilləşmə

ISO/IEC 27001:2013 standartının 10.2 bəndində göstərilən tələblər və 5.1 bəndində müəyyən edilmiş şərh tətbiq edilir.

6 ISO/IEC 27002 standartının əsasında FMİS-ə aid göstərişlər

6.1 Ümumi müddəalar

ISO/IEC 27002:2013-də "informasiya təhlükəsizliyi"ndən bəhs edən təlimatlar potensial şəkildə FEM-in emalının təsir etdiyi şəxsi həyatın toxunulmazlığının qorunmasını əhatə edəcək qədər genişləndirilməlidir.

QEYD 1: Praktikada ISO/IEC 27002:2013-də "informasiya təhlükəsizliyi" anlayışının istifadə olunduğu hallarda onun əvəzinə "informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı" anlayışı nəzərdə tutulur (baxın: Qoşma F).

Bütün nəzarət məqsədləri və nəzarət tədbirləri həm informasiya təhlükəsizliyi ilə bağlı risklər, həm də FEM-in emalı ilə bağlı şəxsi həyatın toxunulmazlığına dair risklər kontekstində nəzərə alınmalıdır.

QEYD 2: Maddə 6-da xüsusi müddəalarla əksi göstərilmədiyi halda və ya tətbiq olunan yurisdiksiyalara əsasən təşkilat tərəfindən müəyyən edilmədiyi halda eyni göstərişlər FEM nəzarətçilərinə və FEM-i emal edən tərəflərə şamil olunur.

6.2 İnformasiya təhlükəsizliyi siyasətləri

6.2.1 İnformasiya təhlükəsizliyi üçün idarəetmə istiqaməti

6.2.1.1 İnformasiya təhlükəsizliyi siyasətləri

ISO/IEC 27002:2013 standartının 5.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyi siyasətlərinə dair 5.1.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat ya şəxsi həyatın toxunulmazlığına dair ayrıca siyasətlər işləyib hazırlamaqla, ya da informasiya təhlükəsizliyi siyasətlərini gücləndirməklə, FEM-in mühafizəsinə dair tətbiq olunan qanunvericiliyə və/və ya normativ aktlara və təşkilat ilə onun tərəfdaşları, onun subpodratçıları və müvafiq üçüncü

tərəfləri (müştərilər, təchizatçılar və s.) arasında razılaşdırılmış və onlar arasında məsuliyyətləri aydın şəkildə bölüşdürən müqavilə əsaslı şərtlərə uyğunluğa nail olmağa yönəlmiş dəstək və məsuliyyətlə bağlı bəyanat hazırlamalıdır.

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyi siyasətlərinə dair 5.1.1 bəndi üçün digər əlavə məlumatlar aşağıdakılardır:

FEM nəzarətçisi və ya FEM-i emal edən tərəf olmasından asılı olmayaraq, FEM-in emalını həyata keçirən hər hansı təşkilat informasiya təhlükəsizliyi siyasətlərinin hazırlanması və saxlanması zamanı FEM-in mühafizəsinə dair tətbiq olunan qanunvericiliyi və/və ya normativ aktları nəzərə almalıdır.

6.2.1.2 İnformasiya təhlükəsizliyi üzrə siyasətlərə baxış

ISO/IEC 27002:2013 standartının 5.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur:

6.3 İnformasiya təhlükəsizliyinin təşkil edilməsi

6.3.1 Daxili struktur

6.3.1.1 İnformasiya təhlükəsizliyinə dair vəzifə və öhdəliklər

ISO/IEC 27002:2013 standartının 6.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyinə dair vəzifələr haqqında 6.1.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat FEM-in emalı ilə bağlı müştərinin istifadə etməsi üçün təmas nöqtəsi müəyyənləşdirməlidir. Təşkilat FEM nəzarətçisi kimi çıxış edərkən, FEM subyektləri üçün onların FEM-in emalı ilə bağlı təmas nöqtəsi müəyyənləşdirin (baxın: 7.3.2).

Təşkilat FEM-in emalı ilə bağlı bütün tətbiq olunan qanunlar və normativ aktlara əməl edilməsini təmin etmək üçün təşkilatın idarəçiliyinin və şəxsi həyatın toxunulmazlığı üzrə proqramın hazırlanması, icrası, texniki xidmətlə təmin edilməsi və monitorinqinə cavabdeh olan bir və ya bir neçə şəxs təyin etməlidir.

Cavabdeh şəxs müvafiq halda aşağıdakıları təmin etməlidir:

— müstəqil olmaq və şəxsi həyatın toxunulmazlığına dair risklərin effektiv idarə edilməsini təmin etmək üçün birbaşa təşkilatın müvafiq rəhbərlik səviyyəsinə hesabat vermək;

— FEM-in emalı ilə əlaqəli bütün məsələlərin idarə edilməsində iştirak etmək;

— məlumatların mühafizəsi üzrə qanunvericilik, normativ aktlar və praktikalar üzrə ekspert olmaq;

— nəzarət orqanları üçün təmas nöqtəsi kimi çıxış etmək;

— təşkilatın yuxarı səviyyəli rəhbərliyini və işçilərini onların FEM-in emalı ilə bağlı öhdəlikləri barədə məlumatlandırmaq;

— təşkilat tərəfindən aparılan şəxsi həyatın toxunulmazlığına təsirlərin qiymətləndirilməsi ilə bağlı məsləhət verməkdir.

QEYD: Bu cür şəxs bəzi yurisdiksiyalarda məlumatların mühafizəsi üzrə məsul şəxs adlanır. Bu yurisdiksiyalar bu cür vəzifənin nə vaxt tələb olunmasını, eləcə də bu şəxsin vəzifə və rolunu müəyyən edir. Bu vəzifə heyət üzvü tərəfindən və ya kənar qaynaqlardan istifadə edilməklə həyata keçirilə bilər.

6.3.1.2 Vəzifə bölgüsü

ISO/IEC 27002:2013 standartının 6.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.3.1.3 Səlahiyyətli qurumlarla əlaqə

ISO/IEC 27002:2013 standartının 6.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.3.1.4 Xüsusi maraq qrupları ilə əlaqə

ISO/IEC 27002:2013 standartının 6.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.3.1.5 Layihələrin idarə olunmasında informasiya təhlükəsizliyi

ISO/IEC 27002:2013 standartının 6.1.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.3.2 Mobil cihazlar və distant iş

6.3.2.1 Mobil cihaz siyasəti

ISO/IEC 27002:2013 standartının 6.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Mobil cihaz siyasəti haqqında 6.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat mobil cihazlardan istifadənin FEM-i təhlükəyə atmamasını təmin etməlidir.

6.3.2.2 Distant iş

ISO/IEC 27002:2013 standartının 6.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.4 Kadrların təhlükəsizliyi

6.4.1 Məşğulluqdan əvvəl

6.4.1.1 Skrininq

ISO/IEC 27002:2013 standartının 7.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.4.1.2 Məşğulluq şərtləri

ISO/IEC 27002:2013 standartının 7.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.4.2 Məşğulluq dövrü

6.4.2.1 Rəhbərliyin məsuliyyətləri

ISO/IEC 27002:2013 standartının 7.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.4.2.2 İnformasiya təhlükəsizliyi üzrə məlumatlılıq, təhsil və təlim

ISO/IEC 27002:2013 standartının 7.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyi üzrə məlumatlılıq, təhsil və təlim haqqında 7.2.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Müvafiq işçi heyətinin şəxsi həyatın toxunulmazlığı və ya təhlükəsizlik qaydalarının və prosedurlarının, xüsusən də FEM ilə məşğul olmağı əhatə edən qayda və prosedurların pozulmasının təşkilat (məs., hüquqi nəticələr, iş və markanın itirilməsi və ya nüfuzuna xələl gəlməsi), heyət (məs., intizam nəticələri) və FEM-in subyekti (məs., fiziki, maddi və emosional nəticələr) üçün mümkün nəticələrindən xəbərdar olmasını təmin etmək üçün tədbirlər, o cümlədən insidentlərin məruzə edilməsi barədə məlumatlılıq tədbirləri həyata keçirilməlidir.

QEYD: Bu cür tədbirlərə FEM-ə çıxış imkanı olan şəxsi heyətin vaxtaşırı keçirilən müvafiq təlimdən yararlanması daxil ola bilər.

6.4.2.3 İntizam prosedurları

ISO/IEC 27002:2013 standartının 7.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.4.3 Məşğulluğun dayandırılması və dəyişməsi

6.4.3.1 Məşğulluğun dayandırılması və ya məşğuluq öhdəliklərinin dəyişdirilməsi

ISO/IEC 27002:2013 standartının 7.3.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5 Aktivlərin idarə edilməsi

6.5.1 Aktivlərə dair məsuliyyət

6.5.1.1 Aktivlərin saxlanması

ISO/IEC 27002:2013 standartının 8.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5.1.2 Aktivlərə sahiblik

ISO/IEC 27002:2013 standartının 8.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5.1.3 Aktivlərdən məqbul istifadə edilməsi

ISO/IEC 27002:2013 standartının 8.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5.1.4 Aktivlərin geri qaytarılması

ISO/IEC 27002:2013 standartının 8.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5.2 Məlumatların təsnifatı

6.5.2.1 Məlumatların təsnifatı

ISO/IEC 27002:2013 standartının 8.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məlumatların təsnifatına dair 8.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilatın məlumatların təsnifatı sistemi FEM-i icra etdiyi planın tərkib hissəsi kimi açıq şəkildə nəzərə almalıdır. Ümumi təsnifat sistemi çərçivəsində FEM-in nəzərə alınması təşkilat tərəfindən hansı FEM-in emal edildiyinin (məs., növ, xüsusi kateqoriyalar), belə FEM-in harada saxlanıldığının və hansı sistemlər vasitəsilə ötürülə biləcəyinin anlaşılmasının ayrılmaz hissəsidir.

6.5.2.2 Məlumatların etiketlənməsi

ISO/IEC 27002:2013 standartının 8.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məlumatların etiketlənməsinə dair 8.2.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat nəzarəti altında olan insanların FEM-in tərifi və FEM adlandırılan məlumatların necə tanınması barədə məlumatlı olmasını təmin etməlidir.

6.5.2.3 Aktivlərin idarə edilməsi

ISO/IEC 27002:2013 standartının 8.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.5.3 Daşıyıcıların idarə edilməsi

6.5.3.1 Silinə bilən daşıyıcının idarə olunması

ISO/IEC 27002:2013 standartının 8.3.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Silinə bilən daşıyıcının idarə olunması haqqında 8.3.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat FEM-in saxlanılması üçün silinə bilən daşıyıcıdan və/və ya cihazlardan hər hansı istifadəni sənədləşdirməlidir. Mümkün olduğu halda təşkilat FEM-i saxlayarkən şifrələməyə icazə verən silinə bilən maddi daşıyıcıdan və/və ya cihazlardan istifadə etməlidir. Şifrələnməmiş daşıyıcı yalnız qaçınılmaz halda istifadə edilməlidir və şifrələnməmiş daşıyıcıdan və/və ya cihazlardan istifadə edildiyi hallarda təşkilat FEM ilə bağlı riskləri azaltmaq üçün prosedurlar və əvəzedici nəzarət tədbirləri (məs., saxtalaşdırmaya qarşı birdəfəlik qablaşdırma) həyata keçirməlidir.

ISO/IEC 27002:2013 standartının Silinə bilən daşıyıcının idarə olunmasına dair 8.3.1 bəndi üçün digər əlavə məlumatlar aşağıdakılardır:

Təşkilatın fiziki sərhədindən kənara çıxarılan silinə bilən daşıyıcı itkiyə, zədələnməyə və icazəsiz çıxış imkanının əldə edilməsinə səbəb ola bilər. Silinə bilən daşıyıcının şifrələnməsi FEM üçün əlavə müdafiə səviyyəsi təmin edir və bu da silinə bilən daşıyıcı təhlükə altında olduqda təhlükəsizlik və şəxsi həyatın toxunulmazlığı risklərini azaldır.

6.5.3.2 Daşıyıcının məhv edilməsi

ISO/IEC 27002:2013 standartının 8.3.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Daşıyıcının məhv edilməsinə dair 8.3.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

FEM-in saxlanıldığı silinə bilən daşıyıcı məhv edildiyi halda sənədləşdirilmiş informasiyaya təhlükəsiz məhv etmə prosedurları daxil edilməli və əvvəlcədən saxlanılan FEM-in əlçatan olmayacağını təmin etmək üçün bu prosedurlar həyata keçirilməlidir.

6.5.3.3 Maddi daşıyıcının ötürülməsi

ISO/IEC 27002:2013 standartının 8.3.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Maddi daşıyıcının ötürülməsinə dair 8.3.3 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Məlumatların ötürülməsi üçün maddi daşıyıcıdan istifadə edilirsə, FEM-i, o cümlədən maddi daşıyıcının növünü, müvafiq icazəyə malik göndərəni/alıcıları, tarix və vaxtı və maddi daşıyıcının sayını ehtiva edən qəbul edilən və göndərilən maddi daşıyıcını qeydə almaq üçün müəyyən sistem qurulmalıdır. İmkan daxilində, məlumatların tranzit deyil, yalnız təyinat nöqtəsində əlçatanlığını təmin etmək üçün şifrələmə kimi əlavə tədbirlər icra olunmalıdır.

Təşkilatın binasından çıxarılmazdan əvvəl FEM-i ehtiva edən maddi daşıyıcı icazələrin verilməsi proseduruna cəlb edilməli və FEM-in müvafiq icazəsi olan heyətdən başqa bir nəfər üçün əlçatan olmaması təmin edilməlidir.

QEYD: Təşkilatın binasından çıxarılan maddi daşıyıcıdakı FEM-in ümumiyyətlə əlçatan olmamasını təmin etməyə yönəlmiş mümkün tədbirlərdən biri müvafiq FEM-i şifrələmək və şifrənin açılması imkanlarını müvafiq icazəyə malik heyətlə məhdudlaşdırmaqdır.

6.6 Çıxış imkanına nəzarət

6.6.1 Çıxış imkanına nəzarətin biznes tələbləri

6.6.1.1 Çıxış imkanına nəzarət siyasəti

ISO/IEC 27002:2013 standartının 9.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.1.2 Şəbəkələrə və şəbəkə xidmətlərinə çıxış

ISO/IEC 27002:2013 standartının 9.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.2 İstifadəçinin çıxış imkanının idarə olunması

6.6.2.1 İstifadəçinin qeydiyyata alınması və qeydiyyatının ləğv edilməsi

ISO/IEC 27002:2013 standartının 9.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İstifadəçinin qeydiyyata alınması və qeydiyyatının ləğv edilməsinə dair 9.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

FEM-in emalı ilə məşğul olan sistemləri və xidmətləri idarə edən və ya işlədən istifadəçilərin qeydiyyata alınması və qeydiyyatının ləğvi prosedurları həmin istifadəçilər üçün istifadəçinin çıxış imkanına nəzarətin təhlükə altında olduğu vəziyyəti (məs., təsadüfən ifşa edilmə nəticəsində şifrələrin və ya digər istifadəçi qeydiyyatı məlumatlarının təhrif olunması və ya təhlükədə olması) nəzərə almalıdır.

Təşkilat FEM-in emalı ilə məşğul olan sistemlər və xidmətlər üçün hər hansı deaktiv olan və ya müddəti bitmiş istifadəçi kimliyini istifadəçilərə yenidən verməməlidir.

Təşkilat FEM-in emalını xidmət kimi təmin etdiyi halda müştəri istifadəçi kimliyinin idarə olunmasının bir neçə və ya bütün aspektlərinə cavabdeh olur. Bu cür hallar sənədləşdirilmiş informasiyaya daxil edilməlidir.

Bəzi yurisdiksiyalar FEM-in emalı ilə məşğul olan sistemlərlə əlaqədar istifadə edilməyən autentifikasiya məlumatlarının yoxlanma tezliyi ilə bağlı xüsusi tələblər qoyur. Bu yurisdiksiyalar çərçivəsində fəaliyyət göstərən təşkilatlar bu tələblərə əməl etməyi nəzərə almalıdır.

6.6.2.2 İstifadəçinin çıxış imkanının təmin edilməsi

ISO/IEC 27002:2013 standartının 9.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İstifadəçinin çıxış imkanının təmin edilməsinə dair 9.2.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat informasiya sisteminə və ona daxil olan FEM-ə çıxışa icazəsi olan istifadəçilər üçün yaradılan istifadəçi profillərinin dəqiq, müasir qeydlərini saxlamalıdır. Bu profil icazə verilən çıxışı təmin edən müəyyənləşdirilmiş texniki nəzarət tədbirlərini icra etmək üçün lazım olan həmin istifadəçi, o cümlədən istifadəçi kimliyi haqqında məlumatlar toplusunu təşkil edir.

Fərdi istifadəçi çıxışı üçün kimliyin tətbiq olunması müvafiq konfiqurasiya olunmuş sistemlərin FEM-ə kimin daxil olduğunu və onların nəyi əlavə etdiyini, sildiyini və ya dəyişdiyini müəyyənləşdirməsinə imkan yaradır. Təşkilatın qorunması ilə yanaşı, istifadəçilər də nəyi emal edib, nəyi emal etmədiklərini müəyyənləşdirə bildikləri üçün qorunurlar.

Təşkilat FEM-in emalını xidmət kimi təmin etdiyi halda müştəri çıxış imkanının idarə olunmasının bir neçə və ya bütün aspektlərinə cavabdeh olur. Müvafiq halda, təşkilat müştərini çıxış imkanının idarə olunmasını həyata keçirmək üçün vasitələr (məs., çıxış imkanını idarə etmək və ya dayandırmaq üçün inzibati hüquqlar təmin etməklə) ilə təmin edir. Bu cür hallar sənədləşdirilmiş informasiyaya daxil edilməlidir.

6.6.2.3 İmtiyazlı çıxış imkanı hüquqlarının idarə olunması

ISO/IEC 27002:2013 standartının 9.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur:

6.6.2.4 İstifadəçilərin gizli autentifikasiya məlumatlarının idarə olunması

ISO/IEC 27002:2013 standartının 9.2.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.2.5 İstifadəçilərin çıxış hüquqlarına baxış

ISO/IEC 27002:2013 standartının 9.2.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.2.6 Çıxış hüquqlarının silinməsi və ya tənzimlənməsi

ISO/IEC 27002:2013 standartının 9.2.6 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.3 İstifadəçinin məsuliyyətləri

6.6.3.1 Gizli autentifikasiya məlumatlarından istifadə

ISO/IEC 27002:2013 standartının 9.3.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.4 Sistemə və tətbiqə çıxışa nəzarət

6.6.4.1 Məlumatlara çıxışın məhdudlaşdırılması

ISO/IEC 27002:2013 standartının 9.4.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.4.2 Təhlükəsiz daxil olma prosedurları

ISO/IEC 27002:2013 standartının 9.4.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Təhlükəsiz daxil olma prosedurları haqqında 9.4.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Müştəri tələb etdiyi halda, təşkilat müştərinin nəzarəti altındakı istənilən istifadəçi hesabları üçün təhlükəsiz daxil olma prosedurlarına şərait yaratmalıdır.

6.6.4.3 Şifrənin idarə olunması sistemi

ISO/IEC 27002:2013 standartının 9.4.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.4.4 Üstün köməkçi proqramlardan istifadə

ISO/IEC 27002:2013 standartının 9.4.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.6.4.5 Proqramın mənbə koduna çıxış imkanına nəzarət

ISO/IEC 27002:2013 standartının 9.4.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.7 Kriptoqrafiya

6.7.1 Kriptoqrafik nəzarət tədbirləri

6.7.1.1 Kriptoqrafik nəzarət tədbirlərindən istifadə siyasəti

ISO/IEC 27002:2013 standartının 10.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Kriptoqrafik nəzarət tədbirlərindən istifadə siyasəti haqqında 10.1.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Bəzi yurisdiksiyalar xüsusi növ FEM-in (məs., sağlamlıqla bağlı məlumatlar, rezidentin qeydiyyat nömrəsi, pasport nömrəsi və sürücülük vəsiqəsinin nömrəsi) mühafizəsi üçün kriptoqrafiyadan istifadə edilməsini tələb edə bilər.

Təşkilat emal etdiyi FEM-i mühafizə etmək üçün kriptoqrafiyadan istifadə etdiyi hallar ilə bağlı müştəriyə məlumat verməlidir. Təşkilat həmçinin müştəriyə təmin etdiyi, öz kriptoqrafik mühafizə vasitələrini tətbiq etməyə kömək edə biləcək hər hansı imkanları barədə də müştəriyə məlumat verməlidir.

6.7.1.2 Kodların idarə edilməsi

ISO/IEC 27002:2013 standartının 10.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8 Fiziki və ətraf mühit təhlükəsizliyi

6.8.1 Təhlükəsiz sahələr

6.8.1.1 Fiziki təhlükəsizlik perimetri

ISO/IEC 27002:2013 standartının 11.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.1.2 Fiziki girişə nəzarət tədbirləri

ISO/IEC 27002:2013 standartının 11.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.1.3 Ofislərin, otaqların və müəssisələrin təhlükəsizliyinin təmin edilməsi

ISO/IEC 27002:2013 standartının 11.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.1.4 Kənar və ətraf mühit təhlükələrinə qarşı müdafiə

ISO/IEC 27002:2013 standartının 11.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.1.5 Təhlükəsiz ərazilərdə iş

ISO/IEC 27002:2013 standartının 11.1.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.1.6 Çatdırılma və yükləmə sahələri

ISO/IEC 27002:2013 standartının 11.1.6 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2 Avadanlıq

6.8.2.1 Avadanlığın yerləşdirilməsi və qorunması

ISO/IEC 27002:2013 standartının 11.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.2 Dəstəkləyici qurğular

ISO/IEC 27002:2013 standartının 11.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.3 Kabel təhlükəsizliyi

ISO/IEC 27002:2013 standartının 11.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.4 Avadanlığa texniki xidmət

ISO/IEC 27002:2013 standartının 11.2.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.5 Aktivlərin silinməsi

ISO/IEC 27002:2013 standartının 11.2.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.6 Binadan kənar avadanlığın və aktivlərin təhlükəsizliyi

ISO/IEC 27002:2013 standartının 11.2.6 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.7 Avadanlığın təhlükəsiz şəkildə məhv edilməsi və ya yenidən istifadəsi

ISO/IEC 27002:2013 standartının 11.2.7 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Avadanlığın təhlükəsiz şəkildə məhv edilməsi və ya yenidən istifadəsi haqqında 11.2.7 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat hər dəfə yaddaş yenidən təyin edildiyi vaxt əvvəllər həmin yaddaşda saxlanılan FEM-in əlçatan olmamasını təmin etməlidir.

İnformasiya sistemində saxlanılan FEM-in silinməsi zamanı performans problemləri həmin FEM-in açıq şəkildə silinməsinin əlverişsiz olduğunu bildirə bilər. Bu da başqa bir istifadəçinin FEM-ə daxil ola bilmə riskini ortaya çıxarır. Xüsusi texniki tədbirlər vasitəsilə bu cür riskin qarşısı alınmalıdır.

Təhlükəsiz məhv edilmə və ya yenidən istifadə zamanı FEM-in saxlanıla biləcəyi yaddaş daşıyıcısını ehtiva edən avadanlıqla sanki FEM ehtiva edirmiş kimi davranılmalıdır.

6.8.2.8 Nəzarətsiz istifadəçi avadanlığı

ISO/IEC 27002:2013 standartının 11.2.8 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.8.2.9 Təmiz masa və təmiz ekran siyasəti

ISO/IEC 27002:2013 standartının 11.2.9 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Təmiz masa və təmiz ekran siyasəti haqqında 11.2.9 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat FEM ehtiva edən çap olunmuş materialın yaradılmasını müəyyənləşdirilmiş emal məqsədini icra etmək üçün lazım olan minimum səviyyəyə qədər məhdudlaşdırmalıdır.

6.9 Əməliyyatların təhlükəsizliyi

6.9.1 Əməliyyat prosedurları və məsuliyyətləri

6.9.1.1 Əməliyyat prosedurlarının sənədləşdirilməsi

ISO/IEC 27002:2013 standartının 12.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.1.2 Dəyişikliklərin idarə edilməsi

ISO/IEC 27002:2013 standartının 12.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.1.3 Potensialın idarə olunması

ISO/IEC 27002:2013 standartının 12.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.1.4 Tərtibat, sınaq və əməliyyat əsaslı mühitlərin ayrılması

ISO/IEC 27002:2013 standartının 12.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.2 Zərərverici proqramlardan qorunma

6.9.2.1 Zərərverici proqramlara qarşı nəzarət tədbirləri

ISO/IEC 27002:2013 standartının 12.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.3 Ehtiyat nüsxənin hazırlanması

6.9.3.1 Məlumatların ehtiyat nüsxəsinin hazırlanması

ISO/IEC 27002:2013 standartının 12.3.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məlumatların ehtiyat nüsxəsinin hazırlanması haqqında 12.3.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat FEM-in ehtiyat nüsxəsinin çıxarılması, geri qaytarılması və bərpası üzrə tələbləri (ümumi məlumatın ehtiyat nüsxəsinin çıxarılması siyasətinin bir hissəsi ola bilər) və ehtiyat nüsxənin çıxarılması tələbləri üçün saxlanılan məlumatlarda ehtiva olunan FEM-in silinməsi üçün hər hansı əlavə tələbləri (məs., müqavilə əsaslı və/və ya qanuni tələblər) əhatə edən siyasətə malik olmalıdır.

Bu baxımdan FEM-ə aid məsuliyyətlər müştəridən asılı ola bilər. Təşkilat müştəriyə ehtiyat nüsxənin çıxarılması ilə bağlı xidmətin məhdudiyyətləri haqqında məlumat verilməsinə əmin olmalıdır.

Təşkilat müştəriləri birbaşa olaraq ehtiyat nüsxənin çıxarılması və bərpa xidmətləri ilə təmin etdiyi halda, o, FEM-in ehtiyat nüsxəsinin çıxarılması və bərpası ilə bağlı müştərilərin imkanları haqqında aydın məlumatı təmin etməlidir.

Bəzi yurisdiksiyalar FEM-in ehtiyat nüsxəsinin çıxarılması tezliyi, ehtiyat nüsxənin çıxarılmasına baxış və yoxlanmasının tezliyi və ya FEM-in geri qaytarılması prosedurları ilə bağlı xüsusi tələblər qoyur. Bu yurisdiksiyalar çərçivəsində fəaliyyət göstərən təşkilatlar bu tələblərə əməl etdiklərini göstərməlidirlər.

FEM-in sistem xətaları, hücum və ya fəlakət səbəbindən bərpa edilməli olduğu vəziyyətlər yarana bilər. FEM bərpa edilərkən (adətən ehtiyat daşıyıcısından) FEM-in etibarlılığının təmin edilə biləcəyi vəziyyətə və/və ya FEM-in qeyri-dəqiqliyi və/və ya natamamlığının müəyyən edildiyi və bunları aradan qaldırmaq üçün proseslərin tətbiq olunduğu vəziyyətə (FEM-in subyektini də cəlb edə bilən) bərpa olunmasını təmin etmək üçün proseslər həyata keçirilməlidir.

Təşkilatın FEM-in bərpası cəhdləri üçün müəyyən proseduru və bu barədə qeydi olmalıdır. FEM-in bərpası cəhdləri haqqında qeyd ən az aşağıdakıları ehtiva etməlidir:

— bərpa prosesinə cavabdeh olan şəxsin adı;

— bərpa edilən FEM-in təsviri.

Bəzi yurisdiksiyalar FEM-in bərpası cəhdləri haqqında qeydlərin məzmununu təyin edir. Təşkilatlar bərpa haqqında qeydlərin məzmunu üçün hər hansı müvafiq yurisdiksiya əsaslı tələblərə uyğunluğu sənədləşdirə bilməlidir. Bu cür müzakirələrin nəticələri sənədləşdirilmiş informasiyaya daxil edilməlidir.

Emal edilən FEM-in təkrar və ya ehtiyat nüsxələrini saxlamaq üçün subpodratçılardan istifadə edilməsi bu sənəddəki subpodrat müqaviləsinə cəlb olunan FEM-in emalı prosesinə tətbiq edilən nəzarət tədbirləri ilə əhatə olunur (baxın: 6.5.3.3, 6.12.1.2). Ehtiyat nüsxənin çıxarılması və bərpa ilə əlaqəli həyata keçirilən maddi daşıyıcı ötürmələri də bu sənəddəki nəzarət tədbirləri ilə əhatə olunur (6.10.2.1).

6.9.4 Qeydiyyat və monitorinq

6.9.4.1 Hadisənin qeydə alınması

ISO/IEC 27002:2013 standartının 12.4.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Hadisənin qeydə alınması haqqında 12.4.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Davamlı və avtomatik monitorinqdən və xəbərdarlıq prosesindən istifadə etməklə, yaxud qeyri-avtomatik üsulla hadisə barədə qeydlərə baxmaq üçün müəyyən proses yaradılmalıdır. Sonuncu halda, uyğunsuzluqları müəyyənləşdirmək və bərpa tədbirləri təklif etmək üçün bu cür baxış müəyyən edilmiş və sənədləşdirilmiş aralıqla icra olunmalıdır.

İmkan daxilində hadisə barədə qeydlər FEM-ə çıxış imkanını, o cümlədən kim tərəfindən, nə vaxt, hansı FEM-in subyektinin FEM-nə daxil olunduğunu və hadisə nəticəsində hansı dəyişikliklərin (əgər varsa) edildiyini (əlavələr, dəyişikliklər və ya silinmələr) qeydə almalıdır.

Xidmətlərin təmin olunmasına çoxsaylı xidmət təminatçıları cəlb olunduğu halda, bu təlimatların icra olunmasında müxtəlif və ya bölüşdürülmüş rollar mövcud ola bilər. Bu rollar aydın şəkildə müəyyənləşdirilməli və sənədləşdirilmiş informasiyaya daxil edilməlidir və təminatçılar arasında hər hansı qeydə çıxış imkanı barədə razılaşma nəzərə alınmalıdır.

FEM-i emal edən tərəflər üçün icra göstərişləri:

Təşkilat qeydə alınan məlumatların müştərilərə təqdim edilib-edilməyəcəyi, nə vaxt təqdim ediləcəyi və ya onlar tərəfindən necə istifadə oluna biləcəyi ilə bağlı meyarları müəyyənləşdirməlidir. Bu meyarlar müştəri üçün əlçatan olmalıdır.

Təşkilat nəzarət etdiyi qeydlərə müştərilərinin çıxışının olmasına icazə verdiyi halda müvafiq nəzarət tədbirləri həyata keçirməlidir. Bunun məqsədi müştərinin yalnız öz fəaliyyətləri ilə bağlı qeydlərə daxil ola bilməsini, onun digər müştərilərin fəaliyyətləri ilə bağlı qeydlərə daxil ola bilməməsini və heç bir yolla qeydlərə düzəliş edə bilməməsini təmin etməkdir.

6.9.4.2 Qeydə alınan məlumatların qorunması

ISO/IEC 27002:2013 standartının 12.4.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Qeydə alınan məlumatların qorunmasına dair 12.4.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Məsələn, təhlükəsizliyin monitorinqi və ya əməliyyat əsaslı diaqnostika üçün qeydə alınan məlumatlar FEM-i ehtiva edə bilər. Qeydə alınan məlumatların yalnız nəzərdə tutulduğu kimi istifadə edilməsini təmin etmək üçün çıxış imkanına nəzarət kimi tədbirlər (baxın: ISO/IEC 27002:2013, 9.2.3) həyata keçirilməlidir.

Qeydə alınan məlumatların saxlama planında müəyyənləşdirildiyi kimi silinməsini, ya da adsızlaşdırılmasını təmin etmək üçün müəyyən prosedur, əsasən də avtomatlaşdırılmış prosedur həyata keçirilməlidir (baxın: 7.4.7).

6.9.4.3 İnzibatçı və operatorun qeydləri

ISO/IEC 27002:2013 standartının 12.4.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.4.4 Saat sinxronizasiyası

ISO/IEC 27002:2013 standartının 12.4.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.5 Əməliyyat əsaslı proqram təminatına nəzarət

6.9.5.1 Əməliyyat sistemlərində proqram təminatının quraşdırılması

ISO/IEC 27002:2013 standartının 12.5.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.6 Texniki həssaslığın idarə olunması

6.9.6.1 Texniki həssas nöqtələrin idarə olunması

ISO/IEC 27002:2013 standartının 12.6.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.6.2 Proqram təminatının quraşdırılması üzrə məhdudiyyət

ISO/IEC 27002:2013 standartının 12.6.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.9.7 İnformasiya sistemlərinin auditi ilə bağlı nəzərə alınmalı məsələlər

6.9.7.1 İnformasiya sistemlərinin auditi üzrə nəzarət tədbirləri

ISO/IEC 27002:2013 standartının 12.7.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10 Kommunikasiya təhlükəsizliyi

6.10.1 Şəbəkə təhlükəsizliyinin idarə edilməsi

6.10.1.1 Şəbəkəyə nəzarət tədbirləri

ISO/IEC 27002:2013 standartının 13.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10.1.2 Şəbəkə xidmətlərində təhlükəsizlik

ISO/IEC 27002:2013 standartının 13.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10.1.3 Şəbəkələrin ayrılması

ISO/IEC 27002:2013 standartının 13.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10.2 Məlumatların ötürülməsi

6.10.2.1 Məlumatların ötürülməsinə dair siyasətlər və prosedurlar

ISO/IEC 27002:2013 standartının 13.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məlumatların ötürülməsinə dair siyasətlər və prosedurlar haqqında 13.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat FEM-in emalı ilə bağlı qaydaların mümkün olduqda, sistemdə və sistemdən kənar tətbiq olunmasını təmin etməyə yönəlmiş prosedurları nəzərə almalıdır.

6.10.2.2 Məlumatların ötürülməsi üçün razılaşmalar

ISO/IEC 27002:2013 standartının 13.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10.2.3 Mesajların elektron ötürülməsi

ISO/IEC 27002:2013 standartının 13.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.10.2.4 Məxfilik və ya məlumatların açıqlanmamasına dair müqavilələr

ISO/IEC 27002:2013 standartının 13.2.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məxfilik və ya məlumatların açıqlanmamasına dair müqavilələr haqqında 13.2.4 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat nəzarəti altındakı və FEM-ə çıxış imkanı olan fərdlərin məxfilik öhdəliyinə tabe olmasını təmin etməlidir. Məxfilik müqaviləsi müqavilənin tərkib hissəsi və ya ayrıca formada olmasından asılı olmayaraq, öhdəliklərə əməl edilməli olan müddəti müəyyənləşdirməlidir.

Təşkilat FEM-i emal edən tərəf kimi çıxış edərkən təşkilat, onun işçiləri və agentləri arasında bağlanan məxfilik müqaviləsi hansı formada olmasından asılı olmayaraq işçilərin və agentlərin məlumatların idarə edilməsi və mühafizəsi ilə bağlı siyasət və prosedurlara əməl etməsini təmin etməlidir.

6.11 Sistemlərin əldə edilməsi, tərtibatı və texniki xidmətlə təmin olunması

6.11.1 İnformasiya sistemlərinin təhlükəsizlik tələbləri

6.11.1.1 İnformasiya təhlükəsizliyi tələblərinin təhlili və spesifikasiyası

ISO/IEC 27002:2013 standartının 14.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.1.2 İctimai şəbəkələr üzrə tətbiq xidmətlərinin təhlükəsizliyinin təmin edilməsi

ISO/IEC 27002:2013 standartının 14.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İctimai şəbəkələr üzrə tətbiq xidmətlərinin təhlükəsizliyinin təmin edilməsi haqqında 14.1.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat etibarsız məlumat ötürmə şəbəkələri vasitəsilə ötürülən FEM-in ötürmə zamanı şifrələnməsini təmin etməlidir.

Etibarsız şəbəkələrə ictimai internet və təşkilatın əməliyyat əsaslı nəzarətindən kənarda olan digər qurğular daxil ola bilər.

QEYD: Bəzi hallarda (məs., e-poçt mübadiləsi) məlumatların ötürüldüyü etibarsız şəbəkə sistemlərinin təbii xüsusiyyətləri effektiv ötürülmə üçün bəzi başlıq və ya trafik məlumatlarının nümayiş etdirilməsini tələb edə bilər.

6.11.1.3 Tətbiq xidmətləri üzrə əməliyyatların qorunması

ISO/IEC 27002:2013 standartının 14.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.2 Tərtibat və dəstək proseslərində təhlükəsizlik

6.11.2.1 Təhlükəsiz tərtibat siyasəti

ISO/IEC 27002:2013 standartının 14.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Təhlükəsiz tərtibat siyasəti haqqında 14.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Sistemin tərtibatı və layihələndirilməsinə yönələn siyasətlər FEM subyektləri qarşısında öhdəliklərə və/və ya hər hansı tətbiq olunan qanunvericiliyə və/və ya normativ aktlara və təşkilatın həyata keçirdiyi emal növlərinə əsaslanaraq, təşkilatın FEM-in emalı ehtiyacları üçün göstərişləri ehtiva etməlidir. Maddə 7 və Maddə 8FEM-in emalı üçün nəzarətlə bağlı nəzərə alınmalı məsələləri təmin edir və bu da sistemlərin layihələndirilməsində şəxsi həyatın toxunulmazlığı üçün siyasətlərin hazırlanmasında faydalı ola bilər.

Layihəyə görə şəxsi həyatın toxunulmazlığı və standart parametrlərə görə şəxsi həyatın toxunulmazlığına töhfə verən siyasətlər aşağıdakı məqamları nəzərə almalıdır:

a) FEM-in mühafizəsinə və proqram təminatının hazırlanması dövründə şəxsi həyatın toxunulmazlığı prinsiplərinin (baxın: ISO/IEC 29100) tətbiq olunmasına dair göstərişlər;

b) layihələndirmə mərhələsində şəxsi həyatın toxunulmazlığı risklərinin qiymətləndirilməsindən və/və ya şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsindən əldə edilən nəticəyə əsaslana bilən şəxsi həyatın toxunulmazlığı və FEM-in mühafizəsi üzrə tələblər (baxın: 7.2.5);

c) Layihənin əsas mərhələlərində FEM-in mühafizəsinə nəzarət mərhələsi;

d) tələb olunan şəxsi həyatın toxunulmazlığı və FEM-in mühafizəsi məlumatları

e) FEM-in emalının standart qaydada azaldılması.

6.11.2.2 Sistemin dəyişməsinə nəzarət prosedurları

ISO/IEC 27002:2013 standartının 14.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.2.3 Əməliyyat platformasında dəyişikliklərdən sonra tətbiqlərə texniki baxış

ISO/IEC 27002:2013 standartının 14.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.2.4 Proqram paketlərinə dəyişikliklər edilməsinə məhdudiyyətlər

ISO/IEC 27002:2013 standartının 14.2.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.2.5 Sistemlərin təhlükəsiz planlaşdırılması prinsipləri

ISO/IEC 27002:2013 standartının 14.2.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Sistemlərin təhlükəsiz planlaşdırılması prinsipləri haqqında 14.2.5 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

FEM-in emalı ilə bağlı sistemlər və/və ya komponentlər layihəyə görə şəxsi həyatın toxunulmazlığı və standart parametrlərə görə şəxsi həyatın toxunulmazlığı prinsiplərinə uyğun olaraq hazırlanmalı və müvafiq nəzarət tədbirlərinin (müvafiq olaraq, FEM nəzarətçiləri və FEM-i emal edən tərəflər üçün Maddə 7 və Maddə 8-də təsvir edildiyi kimi) icrasını proqnozlaşdırmaq və asanlaşdırmaq üçün, xüsusilə də həmin sistemlərdəki FEM-in toplanması və emalı FEM-in emalının müəyyənləşdirilmiş məqsədləri üçün zəruri məqamlarla məhdudlaşdırılacaq formada hazırlanmalıdır (baxın: 7.2).

Məsələn, FEM-in emalını həyata keçirən təşkilat müvafiq yurisdiksiyaya əsasən, FEM-i müəyyən müddətdən sonra məhv etməsinə əmin olmalıdır. Sözügedən FEM-in emalını həyata keçirən sistem bu silmə tələbini asanlaşdıracaq formada hazırlanmalıdır.

6.11.2.6 Təhlükəsiz tərtibat mühiti

ISO/IEC 27002:2013 standartının 14.2.6 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

.

6.11.2.7 Kənar qaynaqların cəlb olunduğu tərtibat prosesi

ISO/IEC 27002:2013 standartının 14.2.7 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Kənar qaynaqların cəlb olunduğu tərtibat prosesi haqqında 14.2.7 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Layihəyə görə şəxsi həyatın toxunulmazlığı və standart parametrlərə görə şəxsi həyatın toxunulmazlığının eyni prinsipləri (baxın: 6.11.2.5) müvafiq halda, kənar qaynaqların cəlb olunduğu informasiya sistemlərinə tətbiq edilməlidir.

6.11.2.8 Sistemin təhlükəsizliyinin sınaqdan keçirilməsi

ISO/IEC 27002:2013 standartının 14.2.8 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.2.9 Sistemin qəbulunun sınaqdan keçirilməsi

ISO/IEC 27002:2013 standartının 14.2.9 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.11.3 Sınaq məlumatları

6.11.3.1 Sınaq məlumatlarının qorunması

ISO/IEC 27002:2013 standartının 14.3.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Sınaq məlumatlarının qorunmasına dair 14.3.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

FEM sınaq məqsədilə istifadə edilməməlidir; uydurma və ya süni hazırlanmış FEM-dən istifadə edilməlidir. FEM-in sınaq məqsədilə istifadə edilməsinin qaçınılmaz ola biləcəyi vəziyyətdə, riskləri mümkün qədər azaltmaq üçün istehsal mühitində istifadə edilən tədbirlərə bərabər olan texniki və təşkilati tədbirlər icra olunmalıdır. Bu cür bərabər tədbirlər mümkün olmadıqda, risklərin qiymətləndirilməsi həyata keçirilməli və müvafiq yumşaldıcı nəzarət tədbirlərinin seçilməsindən məlumatların təmin edilməsi üçün istifadə edilməlidir.

6.12 Təchizatçılarla əlaqələr

6.12.1 Təchizatçılarla əlaqələrdə informasiya təhlükəsizliyi

6.12.1.1 Təchizatçılarla əlaqələr üçün informasiya təhlükəsizliyi siyasətləri

ISO/IEC 27002:2013 standartının 15.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.12.1.2 Təchizatçı müqavilələri çərçivəsində təhlükəsizliyin əhatə edilməsi

ISO/IEC 27002:2013 standartının 15.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Təchizatçı müqavilələri çərçivəsində təhlükəsizliyin əhatə edilməsinə dair 15.1.2 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilat təchizatçılarla müqavilələrdə FEM-in emal edilib-edilməməsi və təşkilatın informasiya təhlükəsizliyi və FEM-in mühafizəsi öhdəliklərini qarşılaması üçün təchizatçının yerinə yetirməli olduğu minimal texniki və təşkilati tədbirləri dəqiqləşdirməlidir (baxın: 7.2.6 və 8.2.1).

Təchizatçılarla müqavilələr emal edilən FEM-in növünü nəzərə alaraq, məsuliyyətləri təşkilat, onun tərəfdaşları, təchizatçıları və müvafiq üçüncü tərəfləri (müştərilər, təchizatçılar və s.) arasında aydın şəkildə bölüşdürməlidir.

Təşkilat və onun təchizatçıları arasında bağlanan müqavilələr təşkilatın tətbiq olunan qanunvericiliyə və/və ya normativ aktlara əməl etməyi dəstəkləməsini və idarə etməsini təmin etməyə yönəlmiş mexanizm təmin etməlidir. Müqavilələr müştərilər üçün məqbul olan, müstəqil şəkildə auditi keçirilən uyğunluğu tələb etməlidir.

QEYD: Bu cür audit məqsədləri üçün müvafiq və tətbiq olunan təhlükəsizlik və şəxsi həyatın toxunulmazlığı standartlarına (məs., ISO/IEC 27001 və ya bu sənəd) uyğunluq nəzərə alına bilər.

FEM-i emal edən tərəflər üçün icra göstərişləri

Təşkilat hər hansı təchizatçı ilə bağlanan müqavilələrdə FEM-in yalnız onun təlimatlarına əsasən emal edilməsini xüsusi olaraq qeyd etməlidir.

6.12.1.3 İnformasiya və kommunikasiya texnologiyaları üzrə təchizat zənciri

ISO/IEC 27002:2013 standartının 15.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.12.2 Təchizatçı xidmətinin təqdim olunmasının idarə edilməsi

6.12.2.1 Təchizatçı xidmətlərinin monitorinqi və onlara baxış

ISO/IEC 27002:2013 standartının 15.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.12.2.2 Təchizatçı xidmətlərinə edilən dəyişikliklərin idarə edilməsi

ISO/IEC 27002:2013 standartının 15.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.13 İnformasiya təhlükəsizliyi üzrə insidentlərin idarə olunması

6.13.1 İnformasiya təhlükəsizliyi üzrə insidentlərin və təkmilləşmələrin idarə olunması

6.13.1.1 Məsuliyyətlər və prosedurlar

ISO/IEC 27002:2013 standartının 16.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Məsuliyyətlər və prosedurlar haqqında 16.1.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Ümumi informasiya təhlükəsizliyi üzrə insidentlərin idarə edilməsi prosesinin tərkib hissəsi kimi təşkilat FEM pozuntularının müəyyənləşdirilməsi və qeydə alınması üçün məsuliyyətlər və prosedurlar müəyyənləşdirməlidir. Bundan əlavə, təşkilat tətbiq olunan qanunvericiliyi və/və ya normativ aktları nəzərə alaraq, FEM pozuntularının (o cümlədən bu cür bildirişlərin bildirilmə vaxtı) müvafiq tərəflərə bildirilməsi və səlahiyyətli orqanlara açıqlanması ilə bağlı məsuliyyətlər və prosedurlar müəyyənləşdirməlidir.

Bəzi yurisdiksiyalar pozuntuya cavab tədbirləri, o cümlədən bildirişlərlə bağlı xüsusi normativ aktlar təyin edir. Bu yurisdiksiyalar çərçivəsində fəaliyyət göstərən təşkilatlar bu normativ aktlara əməl etmələrini nümayiş etdirə bildiklərinə əmin olmalıdırlar.

6.13.1.2 İnformasiya təhlükəsizliyi hadisələrinin məruzə edilməsi

ISO/IEC 27002:2013 standartının 16.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

.

6.13.1.3 İnformasiya təhlükəsizliyinin zəif tərəflərinin məruzə edilməsi

ISO/IEC 27002:2013 standartının 16.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.13.1.4 İnformasiya təhlükəsizliyi hadisələrinin qiymətləndirilməsi və onlarla bağlı qərarlar

ISO/IEC 27002:2013 standartının 16.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.13.1.5 İnformasiya təhlükəsizliyi üzrə insidentlərə cavab

ISO/IEC 27002:2013 standartının 16.1.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyi üzrə insidentlərə cavab haqqında 16.1.5 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

FEM nəzarətçiləri üçün icra göstərişləri

FEM-i ehtiva edən insident cavab tədbirinin görülməsini tələb edən FEM-i ehtiva edən pozuntunun baş verib-vermədiyini müəyyənləşdirmək üçün informasiya təhlükəsizliyi insidentlərinin idarə edilməsi prosesinin tərkib hissəsi kimi təşkilat tərəfindən nəzərdən keçirilməlidir.

Bir hadisənin bu cür nəzərdən keçirilməsi zəruri deyil.

QEYD: 1 İnformasiya təhlükəsizliyi ilə bağlı hadisə mütləq şəkildə FEM-ə və ya təşkilatın FEM-in saxlanıldığı hər hansı avadanlığına və ya qurğularına faktiki icazəsiz çıxış və ya ehtimal edilən icazəsiz çıxışla nəticələnmir. Bunlara şəbəkə mühafizə sistemlərinə və ya kənar serverlərə "ping" və digər yayım hücumları, portun skan edilməsi, uğursuz giriş cəhdləri, xidmətdən imtina hücumu və paket analizi ("packet sniffing") daxil ola bilər, lakin yarana biləcək problemlər sadalananlarla məhdudlaşmır.

FEM ilə bağlı pozuntu baş verərkən cavab prosedurları müvafiq bildirişləri və qeydləri ehtiva etməlidir.

Bəzi yurisdiksiyalar pozuntunun nəzarət orqanlarına və FEM subyektlərinə nə vaxt bildirilməli olduğu halları müəyyənləşdirir.

Bildirişlər aydın olmalıdır və onlar zəruri ola bilər.

QEYD 2 Bildirişlər aşağıdakı kimi təfərrüatları əhatə edə bilər:

— daha çox məlumatın əldə edilə biləcəyi təmas nöqtəsi;

— pozuntunun təsviri və onun gözlənilən nəticələri;

— pozuntunun təsviri, o cümlədən müvafiq fərdlərin sayı, eləcə də müvafiq qeydlərin sayı;

— görülən və ya görülməsi planlaşdırılan tədbirlər.

QEYD 3 Təhlükəsizlik insidentlərinin idarə edilməsi üzrə məlumatlar ISO/IEC 27035 seriyasından əldə edilə bilər.

FEM-i ehtiva edən pozuntu baş verdikdə tənzimləyici və/və ya məhkəmə ilə bağlı məqsədlər üçün hesabat vermək məqsədilə kifayət qədər məlumat ehtiva edən qeyd saxlanılmalıdır, məsələn:

— insidentin təsviri;

— müddəti;

— insidentin nəticələri;

— insidenti məruzə edən şəxsin adı;

— insidentin kimə məruzə edilməsi;

— insidenti həll etmək üçün atılan addımlar (o cümlədən məsul şəxs və bərpa edilən məlumatlar);

— insidentin FEM-in əlçatan olmaması, itməsi, açıqlanması və ya dəyişdirilməsi ilə nəticələnməsi faktı.

FEM-i ehtiva edən pozuntu baş verdiyi halda qeyd müvafiq hallarda təhlükə altında olan FEM-in təsvirini və bildirişlər edilibsə, FEM subyektlərinə, tənzimləyici qurumlara və ya müştərilərə xəbər vermək üçün atılan addımları da ehtiva etməlidir.

FEM-i emal edən tərəflər üçün icra göstərişləri

FEM-i ehtiva edən pozuntunun bildirilməsini əhatə edən müddəalar təşkilat və müştəri arasındakı müqavilənin tərkib hissəsini formalaşdırmalıdır. Müqavilə təşkilatın müştərinin müvafiq səlahiyyətli orqanlara məlumat vermək öhdəliyini qarşılaması üçün ona lazım olan məlumatları necə təmin edəcəyini müəyyənləşdirməlidir. Bu bildiriş öhdəliyi müştərinin və ya FEM-in subyektinin səbəb olduğu və ya onların cavabdeh olduğu sistem komponentləri daxilindəki pozuntunu əhatə etmir. Müqavilə bildirişə cavab müddəti üçün gözlənilən və ya kənardan məcburi olan məhdudiyyətləri də müəyyənləşdirməlidir.

Bəzi yurisdiksiyalarda FEM-i emal edən tərəf pozuntunun olması barədə FEM nəzarətçisinə lazımsız gecikmə olmadan (yəni mümkün qədər tez) və mümkün olarsa pozuntunu aşkar edən kimi məlumat verməlidir ki, FEM nəzarətçisi müvafiq tədbirlər görə bilsin.

FEM-i ehtiva edən pozuntu baş verdikdə tənzimləyici və/və ya məhkəmə ilə bağlı məqsədlər üçün hesabat vermək məqsədilə kifayət qədər məlumat ehtiva edən qeyd saxlanılmalıdır, məsələn:

— insidentin təsviri;

— müddəti;

— insidentin nəticələri;

— insidenti məruzə edən şəxsin adı;

— insidentin kimə məruzə edilməsi;

— insidenti həll etmək üçün atılan addımlar (o cümlədən məsul şəxs və bərpa edilən məlumatlar);

— insidentin FEM-in əlçatan olmaması, itməsi, açıqlanması və ya dəyişdirilməsi ilə nəticələnməsi faktı.

FEM-i ehtiva edən pozuntu baş verdiyi halda qeyd müvafiq hallarda təhlükə altında olan FEM-in təsvirini və bildirişlər edilibsə, müştəriyə və/və ya tənzimləyici qurumlara xəbər vermək üçün atılan addımları da ehtiva etməlidir.

Bəzi yurisdiksiyalarda tətbiq olunan qanunvericilik və/və ya normativ aktlar təşkilatın FEM-i ehtiva edən pozuntu barədə müvafiq tənzimləyici orqanlara (məs., FEM-in mühafizəsi orqanı) birbaşa məlumat verməsini tələb edə bilər.

6.13.1.6 İnformasiya təhlükəsizliyi insidentlərindən nəticə çıxarılması

ISO/IEC 27002:2013 standartının 16.1.6 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.13.1.7 Sübutların toplanması

ISO/IEC 27002:2013 standartının 16.1.7 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur:

6.14 İşin davamlılığının idarə edilməsinin informasiya təhlükəsizliyi aspektləri

6.14.1 İnformasiya təhlükəsizliyinin davamlılığı

6.14.1.1 İnformasiya təhlükəsizliyinin davamlılığının planlaşdırılması

ISO/IEC 27002:2013 standartının 17.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.14.1.2 İnformasiya təhlükəsizliyinin davamlılığının icrası

ISO/IEC 27002:2013 standartının 17.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.14.1.3 İnformasiya təhlükəsizliyinin davamlılığının təsdiqlənməsi, yenilənməsi və qiymətləndirilməsi

ISO/IEC 27002:2013 standartının 17.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.14.2 Məlumat ehtiyatları

6.14.2.1 Məlumatların emalı mexanizmlərinin əlçatanlığı

ISO/IEC 27002:2013 standartının 17.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.15 Uyğunluq

6.15.1 Qanuni və müqavilə əsaslı tələblərə uyğunluq

6.15.1.1 Tətbiq olunan qanunvericilik və müqavilə əsaslı tələblərin müəyyənləşdirilməsi

ISO/IEC 27002:2013 standartının 18.1.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Tətbiq olunan qanunvericilik və müqavilə əsaslı tələblərin müəyyənləşdirilməsi üzrə 18.1.1 bəndi üçün digər əlavə məlumatlar aşağıdakılardır:

Təşkilat FEM-in emalı, o cümlədən birbaşa yerli tənzimləyici orqanın tətbiq etdiyi ciddi məbləğdə pul cərimələri ilə bağlı hər hansı potensial hüquqi sanksiyaları (bəzi öhdəliklərin yerinə yetirilməməsindən qaynaqlana bilən) müəyyənləşdirməlidir. Bəzi yurisdiksiyalarda Beynəlxalq Standartlar belə sənəd kimi təşkilat ilə müştəri arasında bağlanan, onların müvafiq təhlükəsizlik, şəxsi həyatın toxunulmazlığı və FEM-in mühafizəsi məsuliyyətlərini təsvir edən müqavilənin əsasını formalaşdırmaq üçün istifadə oluna bilər. Müqavilənin şərtləri həmin məsuliyyətlərin pozulması zamanı müqavilə əsaslı sanksiyalar üçün əsas təmin edə bilər.

6.15.1.2 Əqli mülkiyyət hüquqları

ISO/IEC 27002:2013 standartının 18.1.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.15.1.3 Qeydlərin mühafizəsi

ISO/IEC 27002:2013 standartının 18.1.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Qeydlərin mühafizəsinə dair 18.1.3 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Cari və keçmiş siyasətlərə və prosedurlara baxış tələb oluna bilər (məs., müştəri mübahisələrinin həlli və nəzarət orqanının həyata keçirdiyi araşdırma hallarında).

Təşkilat şəxsi həyatın toxunulmazlığı siyasətlərinin və müvafiq prosedurların nüsxələrini saxlama planında müəyyənləşdirilən müddət ərzində saxlamalıdır (baxın: 7.4.7). Buna bu sənədlər yenilənəndə onların əvvəlki versiyalarının saxlanılması daxildir.

6.15.1.4 Fərdi eyniləşdirilə bilən məlumatların gizliliyi və mühafizəsi

ISO/IEC 27002:2013 standartının 18.1.4 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.15.1.5 Kriptoqrafik nəzarət tədbirlərinin tənzimlənməsi

ISO/IEC 27002:2013 standartının 18.1.5 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.15.2 İnformasiya təhlükəsizliyinə baxışlar

6.15.2.1 İnformasiya təhlükəsizliyinə müstəqil baxış

ISO/IEC 27002:2013 standartının 18.2.1 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının İnformasiya təhlükəsizliyinə müstəqil baxış haqqında 18.2.1 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təşkilatın FEM-i emal edən tərəf kimi çıxış etdiyi və fərdi müştəri auditlərinin səmərəsiz olduğu və ya təhlükəsizliyə yönəlmiş riskləri artıra bildiyi halda, təşkilat müqavilə bağlamazdan əvvəl və müqavilə müddəti ərzində informasiya təhlükəsizliyinin təşkilatın siyasətlərinə və prosedurlarına uyğun şəkildə icra olunduğuna və idarə edildiyinə dair müstəqil sübutları müştərilərə təqdim etməlidir. Təşkilatın seçdiyi müvafiq müstəqil audit gözlənilən istifadəçilərin ehtiyaclarını qarşılayarsa və nəticələr kifayət qədər şəffaf formada təmin edilərsə, müştərinin təşkilatın məlumatların emalı əməliyyatlarının gözdən keçirilməsi ilə bağlı marağını qarşılamaq üçün adətən məqbul metod olmalıdır.

6.15.2.2 Təhlükəsizlik siyasətlərinə və standartlarına uyğunluq

ISO/IEC 27002:2013 standartının 18.2.2 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar tətbiq olunur.

6.15.2.3 Uyğunluğa texniki baxış

ISO/IEC 27002:2013 standartının 18.2.3 bəndində göstərilən nəzarət və icra üzrə göstərişlər və digər məlumatlar, habelə aşağıdakı əlavə göstərişlər tətbiq olunur:

ISO/IEC 27002:2013 standartının Uyğunluğa texniki baxış haqqında 18.2.3 bəndinin icrası üzrə əlavə göstərişlər aşağıdakılardır:

Təhlükəsizlik siyasətlərinə və standartlarına əməl edilməsinə texniki baxış çərçivəsində təşkilat FEM-in emalı ilə bağlı həmin alətlərin və komponentlərin nəzərdən keçirilməsi metodlarını daxil etməlidir. Buna aşağıdakılar daxil ola bilər:

— yalnız icazə verilən emalın həyata keçirildiyini təsdiqləmək üçün davamlı monitorinq; və/və ya

— xüsusi nüfuzetmə və ya həssaslığın qiymətləndirilməsi sınaqları (məsələn, adsızlaşdırılan məlumatlar toplusu adsızlaşdırma metodlarının təşkilati tələblərlə uyğun olmasını təsdiqləmək üçün "məqsədyönlü hücumçu" sınağına cəlb edilə bilər).

7 FEM nəzarətçiləri üçün ISO/IEC 27002 üzrə əlavə göstərişlər

7.1 Ümumi müddəalar

Maddə 6-da göstərişlər və bu maddədəki əlavələr FEM nəzarətçiləri üçün FMİS-ə aid göstərişləri formalaşdırır. Bu maddədəki sənədləşdirilən icra göstərişləri Qoşma A-da sadalanan nəzarət tədbirləri ilə bağlıdır.

7.2 Məlumatların toplanması və emalı şərtləri

Məqsəd: Emal prosesinin qanuni olduğunu, tətbiq olunan yurisdiksiyalara görə hüquqi əsasının olduğunu və aydın şəkildə müəyyənləşdirilən və qanuni məqsədləri olduğunu müəyyənləşdirmək və sənədləşdirmək.

7.2.1 Məqsədin müəyyənləşdirilməsi və sənədləşdirilməsi

Nəzarət tədbiri

Təşkilat FEM-in emalı üçün xüsusi məqsədləri müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Təşkilat FEM subyektlərinin FEM-in hansı məqsədlə emal edildiyini başa düşmələrini təmin etməlidir. Bunu aydın şəkildə sənədləşdirmək və FEM subyektlərinə çatdırmaq təşkilatın öhdəliyidir. Emalın məqsədi açıq şəkildə bildirilmədən razılıq və seçim adekvat şəkildə verilə bilməz.

FEM-in emalı məqsədinin (məqsədlərinin) sənədləşdirilməsi FEM subyektlərinə təmin ediləcək müvafiq məlumatlarda istifadə edilə biləcək formada, kifayət qədər aydın və ətraflı olmalıdır (baxın: 7.3.2). Buna razılıq almaq üçün zəruri olan məlumatlar (baxın: 7.2.3), eləcə də siyasətlərin və prosedurların qeydləri daxildir (baxın: 7.2.8).

Digər məlumatlar

Bulud hesablama xidmətlərinin yerinə yetirilməsi zamanı ISO/IEC 19944-dəki təsnifat və təriflər FEM-in emalı məqsədini təsvir etmək üçün terminlərin təmin edilməsi baxımından faydalı ola bilər.

7.2.2 Hüquqi əsasın müəyyən edilməsi

Nəzarət tədbiri

Təşkilat FEM-in müəyyənləşdirilən məqsədlər çərçivəsində emalı üçün müvafiq hüquqi əsası müəyyənləşdirməli, sənədləşdirməli və ona əməl etməlidir.

İcra göstərişləri

Bəzi yurisdiksiyalarda təşkilatın emal prosesindən əvvəl emal prosesinin qanuniliyinin lazımi qaydada müəyyənləşdirildiyini göstərə bilməsi tələb edilir.

FEM-in emalının hüquqi əsasına aşağıdakılar daxil ola bilər:

— FEM subyektlərindən alınan razılıq;

— müqavilənin icrası;

— qanuni öhdəliyə uyğunluq;

— FEM subyektlərinin ən mühüm maraqlarının qorunması;

— ictimai marağa görə həyata keçirilən tapşırığın səmərəliliyi;

— FEM nəzarətçisinin qanuni maraqları.

Təşkilat hər bir FEM-in emalı fəaliyyəti üçün bu əsası sənədləşdirməlidir (baxın: 7.2.8).

Təşkilatın qanuni maraqlarına məsələn, şəxsi həyatın toxunulmazlığının qorunması ilə bağlı FEM subyektləri qarşısındakı öhdəliklər ilə tarazlaşdırılmalı olan informasiya təhlükəsizliyi məqsədləri daxil ola bilər.

FEM-in xüsusi kateqoriyaları FEM-in xarakterinə görə (məs., sağlamlıqla bağlı məlumatlar), ya da müvafiq FEM subyektləri tərəfindən (məs., uşaqlarla bağlı FEM) müəyyənləşdirildikdə təşkilat bu FEM kateqoriyalarını özünün təsnifat sisteminə daxil etməlidir.

Bu kateqoriyalara aid olan FEM təsnifatı bir yurisdiksiyadan digərinə görə dəyişə bilər və müxtəlif biznes növlərinə tətbiq edilən müxtəlif tənzimləyici rejimlər arasında fərqli ola bilər, buna görə də təşkilat həyata keçirilməkdə olan FEM-in emal prosesinə tətbiq olunan təsnifat (təsnifatlar) barədə məlumatlı olmalıdır.

FEM-in xüsusi kateqoriyalarının istifadəsi həmçinin daha ciddi nəzarət tədbirlərinə məruz qala bilər.

FEM-in emalı məqsədlərinin dəyişməsi və ya genişləndirilməsi hüquqi əsasın yenilənməsini və/və ya ona yenidən baxılmasını tələb edə bilər. O, FEM-in subyektindən əlavə razılığın alınmasını da tələb edə bilər.

7.2.3 Razılığın nə vaxt və necə alınacağının müəyyən edilməsi

Nəzarət tədbiri

Təşkilat FEM-in emalı üçün FEM subyektlərindən razılıq alınıb-alınmadığını, nə vaxt və necə alındığını göstərə biləcəyi müəyyən proses müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Digər qanuni əsaslar tətbiq edilməsə, FEM-in emalı üçün razılıq tələb oluna bilər. Təşkilat razılığın nə vaxt alınmalı olduğunu və razılığın alınmasına dair tələbləri açıq şəkildə sənədləşdirməlidir. emal prosesinin məqsədinin (məqsədlərinin) razılığın alınıb-alınmadığı və necə alındığı ilə bağlı məlumatlarla əlaqələndirilməsi faydalı ola bilər.

Bəzi yurisdiksiyalarda razılığın necə alınması və qeydə alınması ilə bağlı xüsusi tələblər var (məs., digər müqavilələrdən ayrı şəkildə). Bundan əlavə, məlumatların toplanılmasının müəyyən növləri (məsələn, elmi tədqiqat üçün) və müəyyən növ FEM subyektləri (məs., uşaqlar) əlavə tələblərə məruz qala bilər. Təşkilat bu cür tələbləri nəzərə almalı və razılıq mexanizmlərinin həmin tələbləri necə qarşıladığını sənədləşdirməlidir.

7.2.4 Razılığın əldə edilməsi və qeydə alınması

Nəzarət tədbiri

Təşkilat sənədləşdirilən proseslərə əsasən FEM subyektlərindən razılıq almalı və razılığı qeyd etməlidir.

İcra göstərişləri

Təşkilat FEM subyektlərindən razılığı tələb üzrə verilən razılığın təfərrüatlarını təmin edə biləcək formada almalı və qeyd etməlidir (məsələn, razılığın verildiyi vaxt, FEM-in subyektinin eyniləşdirilməsi və razılıq bəyanatı).

Razılıq prosesindən əvvəl FEM-in subyektinə təqdim edilən məlumatlar 7.3.3 bəndindəki göstərişlərə uyğun olmalıdır.

Razılıq aşağıdakı kimi olmalıdır:

— sərbəst şəkildə verilən;

— emal prosesinin məqsədinə uyğun olaraq spesifik; və

— dəqiq və aydın.

7.2.5 Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi

Nəzarət tədbiri

Təşkilat FEM-in yeni emal prosesi və ya FEM-in mövcud emal prosesinə dəyişikliklər planlaşdırılarkən şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi ehtiyaclarını qiymətləndirməli və müvafiq olduqda icra etməlidir.

İcra göstərişləri

FEM-in emalı FEM subyektləri üçün risklər yaradır. Bu risklər şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi yolu ilə qiymətləndirilməlidir. Bəzi yurisdiksiyalarda şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsinin məcburi olduğu hallar müəyyənləşdirilir. Meyarlara FEM subyektlərinə hüquqi təsir edən avtomatik qərar qəbulu, FEM-in xüsusi kateqoriyalarının geniş miqyaslı emalı (məs., sağlamlıqla bağlı məlumatlar, irqi və ya etnik mənsubiyyət, siyasi əqidələr, dini və ya fəlsəfi inanclar, həmkarlar ittifaqına üzvlük, genetik məlumatlar və ya biometrik məlumatlar) və ya ictimai cəhətdən əlçatan sahədə geniş miqyasda sistemli monitorinq daxil ola bilər.

Təşkilat şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsinin tamamlanması üçün zəruri olan elementləri müəyyənləşdirməlidir. Bunlara emal edilən FEM-in növlərinin, FEM-in harada saxlanıldığının və haraya ötürülə biləcəyinin siyahısı daxil ola bilər. Məlumatların axını üzrə diaqramlar və məlumat xəritələri də bu kontekstdə faydalı ola bilər (şəxsi həyatın toxunulmazlığına təsirlərin və ya digər risklərin qiymətləndirilməsində istifadə oluna biləcək FEM-in emalı ilə bağlı qeydlərin təfərrüatlarını öyrənmək üçün baxın: 7.2.8).

Digər məlumatlar

FEM-in emalı ilə bağlı şəxsi həyatın toxunulmazlığına təsirlərin qiymətləndirilməsinə dair göstərişlər ISO/IEC 29134 standartından əldə edilə bilər.

7.2.6 FEM-i emal edən tərəflərlə müqavilələr

Nəzarət tədbiri

Təşkilat istifadə etdiyi hər hansı FEM-i emal edən tərəflə yazılı müqavilə bağlamalı və FEM-i emal edən tərəflərlə müqavilələrinin Qoşma B-dəki müvafiq nəzarət tədbirlərinin icrasını əhatə etməsini təmin etməlidir.

İcra göstərişləri

Təşkilat ilə onun adından FEM-in emalını həyata keçirən hər hansı FEM-i emal edən tərəf arasında bağlanan müqavilə FEM-i emal edən tərəfin informasiya təhlükəsizliyinə yönəlmiş risklərin qiymətləndirilməsi prosesini (baxın: 5.4.1.2) və FEM-i emal edən tərəfin həyata keçirdiyi FEM-in emalı prosesinin əhatə dairəsini (baxın: 6.12) nəzərə alaraq, Qoşma B-də müəyyənləşdirilən müvafiq nəzarət tədbirlərini icra etməsini tələb etməlidir. Standart olaraq, Qoşma B-də müəyyənləşdirilən bütün nəzarət tədbirlərinin münasib olduğu qəbul edilməlidir. Təşkilat FEM-i emal edən tərəfin Qoşma B-dəki nəzarət tədbirini icra etməsini tələb etməməyə qərar verirsə, həmin nəzarət tədbirinin istisna edilməsini əsaslandırmalıdır (baxın: 5.4.1.3).

Müqavilə hər bir tərəfin məsuliyyətlərini fərqli şəkildə müəyyənləşdirə bilər, lakin bu sənədə uyğun olmaq üçün bütün nəzarət tədbirləri nəzərə alınmalı və sənədləşdirilmiş informasiyaya daxil edilməlidir.

7.2.7 Birgə FEM nəzarətçisi

Nəzarət tədbiri

Təşkilat FEM-in hər hansı birgə FEM nəzarətçisi ilə birgə emalına (o cümlədən FEM-in mühafizəsi və təhlükəsizlik tələbləri) dair müvafiq vəzifə və öhdəlikləri müəyyənləşdirməlidir.

İcra göstərişləri

FEM-in emalı ilə bağlı vəzifə və öhdəliklər şəffaf formada müəyyənləşdirilməlidir.

Bu vəzifə və öhdəliklər FEM-in birgə emalı üzrə şərtləri ehtiva edən müqavilədə və ya hər hansı bənzər hüquqi öhdəlik yaradan sənəddə sənədləşdirilməlidir (əsaslandırılmalıdır). Bəzi yurisdiksiyalarda belə müqavilə məlumatların paylaşılması müqaviləsi adlanır.

Birgə FEM nəzarətçisi ilə müqaviləyə aşağıdakılar daxil ola bilər (bu siyahı nə tam, nə də müfəssəl deyil):

— FEM-in paylaşılmasının / birgə FEM nəzarətçisi ilə əlaqənin məqsədi;

— birgə FEM nəzarətçisi ilə əlaqənin tərkib hissəsi olan təşkilatların (FEM nəzarətçilərinin) kimliyi;

— müqavilə çərçivəsində paylaşılacaq və/və ya ötürüləcək və emal ediləcək FEM kateqoriyaları;

— emal əməliyyatlarının icmalı (məs., ötürülməsi, istifadəsi);

— müvafiq vəzifə və məsuliyyətlərin təsviri;

— FEM-in mühafizəsi üçün texniki və təşkilati təhlükəsizlik tədbirlərinin icrasına dair məsuliyyət;

— FEM ilə bağlı pozuntu baş verdiyi zaman öhdəliyin təsviri (məs., pozuntu barədə kimin, nə vaxt bildirəcəyi, qarşılıqlı informasiya);

— FEM-in saxlanılması və/və ya məhv edilməsi şərtləri;

— müqaviləyə əməl edilməməsi halında öhdəliklər;

— FEM subyektləri qarşısında öhdəliklərin necə qarşılanması;

— Birgə FEM nəzarətçiləri arasındakı razılığın mahiyyətini əhatə edən məlumatların FEM subyektlərinə necə təmin ediləcəyi;

— FEM subyektlərinin əldə etmək hüquqlarının olduğu digər məlumatları necə əldə edə biləcəyi; və

— FEM subyektləri üçün təmas nöqtəsi.

7.2.8 FEM-in emalı ilə əlaqəli qeydlər

Nəzarət tədbiri

Təşkilat FEM-in emalına dair öhdəliklərinin dəstəklənməsi üçün zəruri qeydləri müəyyənləşdirməli və onları təhlükəsiz şəkildə saxlamalıdır.

İcra göstərişləri

FEM-in emalına dair qeydlərin saxlanmasının üsullarından biri təşkilatın həyata keçirdiyi FEM-in emal fəaliyyətləri üzrə reyestrə və ya siyahıya sahib olmaqdır. Bu cür reyestrə aşağıdakılar daxil ola bilər:

— emalın növü;

— emalın məqsədləri;

— FEM kateqoriyalarının və FEM subyektlərinin (məs., uşaqlar) təsviri;

— FEM-in açıqlandığı və ya açıqlanacağı resipiyentlərin, o cümlədən üçüncü ölkələrdəki və ya beynəlxalq təşkilatlardakı resipiyentlərin kateqoriyaları;

— texniki və təşkilati təhlükəsizlik tədbirlərinin ümumi təsviri; və

— Şəxsi həyatın toxunulmazlığına Təsirin Qiymətləndirilməsi hesabatı.

Bu cür reyestrin dəqiqliyinə və tamlığına cavabdeh olan şəxs olmalıdır.

7.3 FEM subyektləri qarşısında öhdəliklər

Məqsəd: FEM subyektlərinə onların FEM-nin emalı barədə müvafiq məlumatların verilməsini təmin etmək və FEM subyektləri qarşısında FEM-in emalı ilə bağlı hər hansı digər müvafiq öhdəlikləri qarşılamaq.

7.3.1 FEM subyektləri qarşısında öhdəliklərin müəyyən edilməsi və yerinə yetirilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərinin FEM-nin emalı ilə bağlı onların qarşısında hüquqi, normativ və iş öhdəliklərini müəyyənləşdirməli və sənədləşdirməli və bu öhdəlikləri qarşılayacaq vasitələri təmin etməlidir.

İcra göstərişləri

FEM subyektləri qarşısında öhdəliklər və onları dəstəkləyəcək vasitələr bir yurisdiksiyadan digərinə görə dəyişir.

Təşkilat FEM subyektlərinin qarşısındakı öhdəlikləri qarşılamaq üçün müvafiq vasitələri əlçatan formada və vaxtında təmin etməsinə əmin olmalıdır. FEM subyektləri üçün təşkilatın onların qarşısındakı öhdəliklərini hansı ölçüdə və necə yerinə yetirdiyini təsvir edən aydın sənədlər və onların öz tələblərini bildirə biləcəyi müasir təmas nöqtəsi təmin edilməlidir.

Təmas nöqtəsi FEM toplamaq və razılıq əldə etmək üçün istifadə edilən üsula bənzər şəkildə təmin edilməlidir (məs., FEM e-poçt və ya veb-sayt vasitəsilə toplanılırsa, təmas nöqtəsi də telefon və ya faks kimi alternativ yolla deyil, e-poçt və ya veb-sayt ilə təmin edilməlidir).

7.3.2 FEM subyektləri üçün məlumatların müəyyən edilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərinə öz FEM-nin emalı ilə bağlı veriləcək məlumatları və bu cür təminatın vaxtını müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Təşkilat FEM subyektlərinə məlumatların nə vaxt veriləcəyinə (məs., emal prosesindən əvvəl, tələb olunduğu vaxtdan etibarən müəyyən müddət ərzində və s.) və veriləcək məlumatların növünə dair hüquqi, normativ və/və ya iş tələblərini müəyyənləşdirməlidir.

Tələblərdən asılı olaraq, məlumatlar bildiriş formasında ola bilər. FEM subyektlərinə təmin edilə biləcək məlumat növlərinə nümunə olaraq aşağıdakılar verilə bilər:

— emalın məqsədi barədə məlumatlar;

— FEM nəzarətçisi və ya onun nümayəndəsinin əlaqə məlumatları;

— emal prosesinin hüquqi əsası barədə məlumatlar;

— FEM birbaşa FEM-in subyektindən alınmayıbsa, haradan əldə edildiyi barədə məlumatlar;

— FEM-in təmin edilməsinin qanunla müəyyən edilmiş və ya müqavilə əsaslı tələb olub-olmaması və müvafiq olduqda, FEM-in təmin edilməməsinin mümkün nəticələri barədə məlumatlar;

— FEM subyektləri qarşısında 7.3.1 bəndində müəyyən edilən öhdəliklər və FEM subyektlərinin xüsusən öz FEM-nə daxil olmaq, onu dəyişdirmək, düzəltmək, silinməsini tələb etmək, FEM-nin bir nüsxəsini almaq və emal prosesinə etiraz etmək məsələlərində bu öhdəliklərdən necə faydalana biləcəyi barədə məlumatlar;

— FEM-in subyektinin razılığını necə geri götürə biləcəyinə dair məlumatlar;

— FEM-in ötürülməsi əməliyyatları barədə məlumatlar;

— FEM-in resipiyentləri və ya resipiyent kateqoriyaları barədə məlumatlar;

— FEM-in saxlanılacağı müddət barədə məlumatlar;

— FEM-in avtomatik emalına əsaslanan avtomatik qərar qəbulundan istifadə barədə məlumatlar;

— şikayətin bildirilməsi hüququ və bu cür şikayətin necə bildiriləcəyi barədə məlumatlar;

— məlumatların təmin edilmə tezliyi ilə bağlı məlumatlar (məs., "vaxtında edilən" bildiriş, təşkilatın müəyyən etdiyi tezlik və s.).

Təşkilat FEM-in emalı məqsədlərinin dəyişildiyi və ya genişləndirildiyi halda yenilənmiş məlumatları təmin etməlidir.

7.3.3 FEM subyektlərinə məlumatların təqdim edilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərini FEM nəzarətçisini eyniləşdirən və onların FEM-nin emalını təsvir edən aydın və asanlıqla əlçatan məlumatlarla təmin etməlidir.

İcra göstərişləri

Təşkilat 7.3.2 bəndində verilən məlumatları FEM subyektlərinə vaxtında, yığcam, tam, şəffaf, başa düşülən və asanlıqla əlçatan formada, hədəf auditoriyaya uyğun olaraq aydın və sadə dildən istifadə edərək təmin etməlidir.

Müvafiq halda məlumatlar FEM-in toplanılması zamanı təqdim edilməlidir. O, həmçinin daima əlçatan olmalıdır.

QEYD: Təsvirlər və şəkillər nəzərdə tutulan emal prosesinin vizual icmalını təqdim etməklə FEM-in subyekti üçün faydalı ola bilər.

7.3.4 Razılığın dəyişdirilməsi və ya geri götürülməsi mexanizminin təmin edilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərini razılıqlarını dəyişdirmək və ya geri götürmək üçün mexanizm təmin etməlidir.

İcra göstərişləri

Təşkilat FEM subyektlərinə razılıqlarını istənilən vaxt geri götürmək hüquqları (yurisdiksiyalara görə dəyişə bilər) barədə məlumat verməli və bunu həyata keçirmək üçün mexanizm təmin etməlidir. Razılığın geri götürülməsi üçün istifadə edilən mexanizm sistemdən asılıdır; o, mümkün olduqda razılığın alınması mexanizmləri ilə uyğun olmalıdır. Məsələn, razılıq e-poçt və ya veb-sayt vasitəsilə alınırsa, razılığın geri götürülməsi üçün mexanizm də eyni olmalı, telefon və ya faks kimi alternativ mexanizm olmamalıdır.

Razılığı dəyişdirməyə FEM-in emalı prosesinə məhdudiyyətlərin qoyulması daxil ola bilər və bu məhdudiyyətlər bəzi hallarda FEM nəzarətçisinin FEM-i silməsini məhdudlaşdırmağı ehtiva edə bilər.

Bəzi yurisdiksiyalarda FEM-in subyektinin öz razılığını nə vaxt və necə dəyişdirə və ya geri götürə biləcəyinə dair məhdudiyyətlər tətbiq edilir.

Təşkilat razılığın geri götürülməsi və ya dəyişdirilməsi üzrə hər hansı tələbi razılığın qeydə alınması üsuluna bənzər formada qeydə almalıdır.

Razılığa hər hansı şəkildə dəyişiklik edilməsi uyğun sistemlər vasitəsilə müvafiq icazəyə malik istifadəçilərə və müvafiq üçüncü tərəflərə bildirilməlidir.

Təşkilat cavab müddəti müəyyən etməli və müraciətlər ona uyğun olaraq idarə edilməlidir.

Əlavə məlumatlar

FEM-in müəyyən şəkildə emalı üçün razılıq geri götürülərkən razılığın geri götürülməsindən əvvəl icra edilən bütün FEM-in emalı əməliyyatları adətən müvafiq şəkildə nəzərə alınmalıdır, lakin bu cür emal prosesinin nəticələri yeni emal üçün istifadə edilməməlidir. Məsələn, FEM-in subyekti profilləşdirmə üçün verdiyi razılığı geri götürərsə, onun profili artıq istifadə olunmamalı və ya ona müraciət edilməməlidir.

7.3.5 FEM-in emalına etiraz mexanizminin təmin edilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərini öz FEM-nin emalına etiraz etmək üçün mexanizmlə təmin etməlidir.

İcra göstərişləri

Bəzi yurisdiksiyalarda FEM subyektlərinə öz FEM-nin emalına etiraz etmək hüququ verilir. Belə yurisdiksiyaların qanunvericiliyinə və/və ya normativ aktlarına tabe olan təşkilatlar FEM subyektlərinin bu hüquqdan istifadə etməsinə imkan verməк üçün müvafiq tədbirləri icra etmələrinə əmin olmalıdır.

Təşkilat FEM subyektlərinin emal prosesinə etirazları ilə bağlı hüquqi və normativ tələbləri sənədləşdirməlidir (məs., FEM-in birbaşa marketinq məqsədilə emalı ilə bağlı etiraz). Təşkilat subyektlərə bu vəziyyətlərdə etiraz etmək imkanı ilə bağlı məlumat verməlidir. Etiraz etmək mexanizmləri dəyişə bilər, lakin o, təmin edilən xidmətin növü ilə uyğun olmalıdır (məs., onlayn xidmətlər bu imkanı onlayn formada təmin etməlidir).

7.3.6 Məlumatlara çıxış imkanı, onların düzəldilməsi və/və ya silinməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərinin öz FEM-nə daxil olması, düzəliş etməsi və/və ya silməsi öhdəliklərini qarşılamaq üçün siyasətlər, prosedurlar və/və ya mexanizmlər tətbiq etməlidir.

İcra göstərişləri

Təşkilat FEM subyektlərinin tələb edildiyi halda və lazımsız gecikmə olmadan öz FEM-nə çıxış əldə etməsinə, düzəliş etməsinə və silməsinə imkan yaradan siyasətlər, prosedurlar və/və ya mexanizmlər tətbiq etməlidir.

Təşkilat cavab müddəti müəyyən etməli və müraciətlər ona uyğun olaraq idarə edilməlidir.

Hər hansı düzəlişlər və ya silinmələr sistem vasitəsilə və/və ya müvafiq icazəyə malik istifadəçilərə bildirilməli və FEM-in ötürüldüyü üçüncü tərəflərə (baxın: 7.3.7) göndərilməlidir.

QEYD: 7.5.3 bəndində müəyyənləşdirilən nəzarət tədbiri nəticəsində yaradılan qeydlər bu baxımdan kömək ola bilər.

Təşkilat FEM-in subyektinin məlumatların dəqiqliyi və ya düzəldilməsi ilə bağlı mübahisə yarada biləcəyi halda istifadə ediləcək siyasətlər, prosedurlar və/və ya mexanizmlər tətbiq etməlidir. Bu siyasətlər, prosedurlar və/və ya mexanizmlər hansı dəyişikliklərin edildiyi və düzəlişlərin edilmənin mümkün olmaması səbəbləri (bu hal baş verdikdə) barədə FEM-in subyektinə məlumat verilməsini ehtiva etməlidir.

Bəzi yurisdiksiyalarda FEM-in subyektinin öz FEM-nə düzəliş etməsini və ya onu silməsini nə vaxt və necə tələb edə biləcəyinə məhdudiyyətlər qoyulur. Təşkilat bu məhdudiyyətləri müvafiq formada müəyyənləşdirməli və onlar barədə yeniliklərlə bağlı məlumatlı olmalıdır.

7.3.7 FEM nəzarətçilərinin üçüncü tərəfləri məlumatlandırmaq öhdəlikləri

Nəzarət tədbiri

Təşkilat FEM-in paylaşıldığı üçüncü tərəfləri paylaşılan FEM-lə bağlı hər hansı dəyişiklik, razılığın geri götürülməsi və ya etirazlar barədə məlumatlandırmalı və bunu həyata keçirmək üçün müvafiq siyasətlər, prosedurlar və/və ya mexanizmlər icra etməlidir.

İcra göstərişləri

Təşkilat mövcud texnologiyanı nəzərə alaraq, paylaşılan FEM ilə bağlı hər hansı razılığın dəyişilməsi və ya geri götürülməsi və ya etirazlar barədə üçüncü tərəfləri məlumatlandırmaq üçün müvafiq addımlar atmalıdır. Bəzi yurisdiksiyalarda bu fəaliyyətlərin bu üçüncü tərəflərə bildirilməsinə dair hüquqi tələb qoyulur.

Təşkilat üçüncü tərəflərlə fəal ünsiyyət kanalları müəyyənləşdirməli və saxlamalıdır. Onların icrası və qorunub saxlanılmasından məsul olan fərdlərə müvafiq məsuliyyətlər təyin edilə bilər. Təşkilat üçüncü tərəfləri məlumatlandırarkən onların məlumatı qəbul etdiklərini təsdiq etmələrini izləməlidir.

QEYD: FEM subyektləri qarşısında öhdəliklərdən qaynaqlanan dəyişikliklərə FEM-in subyektinin tələb etdiyi kimi razılığın dəyişilməsi və ya geri götürülməsi, düzəliş, silmə və ya emal məhdudiyyətləri barədə müraciətlər və ya FEM-in emalına etirazlar daxildir.

7.3.8 Emal edilən FEM-in surətinin təmin edilməsi

Nəzarət tədbiri

Təşkilat FEM-in subyekti tələb etdikdə emal edilən FEM-in surətini təmin edə bilməlidir.

İcra göstərişləri

Təşkilat emal edilən FEM-in surətini FEM-in subyektinin əldə edə biləcəyi strukturlu, geniş şəkildə istifadə edilə bilən formatda təmin etməlidir.

Bəzi yurisdiksiyalar təşkilatın emal edilən FEM-in surətini FEM-in subyektinin və ya resipiyent FEM nəzarətçisinin ötürə bilməyinə imkan verən formada təmin etməli olduğu halları müəyyənləşdirir (adətən strukturlu, geniş istifadə edilə bilən və maşınla oxuna bilən formatda).

Təşkilat FEM-in subyektinə verilən FEM-in hər hansı nüsxələrinin xüsusi olaraq həmin FEM-in subyekti ilə bağlı olmağından əmin olmalıdır.

Tələb edilən FEM saxlanılma və məhv edilmə siyasətinə (7.4.7 bəndində təsvir edildiyi kimi) əsasən artıq silindiyi halda, FEM nəzarətçisi FEM-in subyektinə tələb olunan FEM-in artıq silindiyi barədə məlumat verməlidir.

Təşkilatın artıq FEM-in subyektini eyniləşdirə bilmədiyi hallarda (məs., adsızlaşdırma prosesinin nəticəsi kimi) təşkilat təkcə bu nəzarət tədbirinin icra edilməsinə görə FEM subyektlərini eyniləşdirməyə (yenidən eyniləşdirməyə) çalışmamalıdır. Lakin bəzi yurisdiksiyalarda qanuni müraciətlər yenidən eyniləşdirmə və daha sonra məlumatların açıqlanmasına imkan yaratmaq üçün FEM-in subyektindən əlavə məlumatların istənilməsini tələb edə bilər.

Texniki cəhətdən mümkün olduqda, FEM-in surətinin FEM-in subyektinin sorğusu əsasında bir təşkilatdan birbaşa digər təşkilata ötürülməsi mümkün olmalıdır.

7.3.9 Müraciətlərin emal edilməsi

Nəzarət tədbiri

Təşkilat FEM subyektlərinin qanuni müraciətlərinin idarə edilməsinə və ona cavab verilməsinə yönəlmiş siyasətləri və prosedurları müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Qanuni müraciətlərə emal edilən FEM-in surətinə dair müraciətlər və ya şikayətin bildirilməsinə dair müraciətlər daxil ola bilər.

Bəzi yurisdiksiyalar təşkilata müəyyən hallarda ödəniş tutmağa icazə verir (məs., izafi və ya təkrar müraciətlər olduqda).

Müraciətlər müvafiq müəyyən edilən cavab müddəti ərzində emal edilməlidir.

Bəzi yurisdiksiyalar müraciətlərin mürəkkəbliyindən və sayından asılı olaraq, cavab müddətini, eləcə də FEM subyektlərini hər hansı gecikmə barədə məlumatlandırma tələblərini müəyyənləşdirir. Müvafiq cavab müddəti şəxsi həyatın toxunulmazlığı siyasətində müəyyənləşdirilməlidir.

7.3.10 Avtomatik qərar qəbulu

Nəzarət tədbiri

Təşkilat yalnız FEM-in avtomatik emalına əsaslanan və təşkilatın FEM-in subyekti ilə bağlı verdiyi qərarlardan qaynaqlanan FEM subyektləri qarşısındakı öhdəlikləri, o cümlədən hüquqi öhdəlikləri müəyyənləşdirməli və nəzərə almalıdır.

İcra göstərişləri

Bəzi yurisdiksiyalar yalnız FEM-in avtomatik emalına əsaslanan qərar FEM subyektlərinə ciddi şəkildə təsir etdiyi halda onlar qarşısında öhdəlikləri müəyyənləşdirir (məs., avtomatik qərar qəbulunun olmasının bildirilməsi, FEM subyektlərinin bu cür qərar qəbuluna etiraz etməsinə imkan verilməsi və /və ya insan müdaxiləsindən istifadə).

QEYD: Bəzi yurisdiksiyalarda bəzi FEM-in emalı əməliyyatların tam şəkildə avtomatlaşdırılması mümkün olmur.

Bu yurisdiksiyalar çərçivəsində fəaliyyət göstərən təşkilatlar bu öhdəliklərə əməl etməyi nəzərə almalıdır.

7.4 Layihəyə görə və standart parametrlərə görə şəxsi həyatın toxunulmazlığı

Məqsəd: Proseslərin və sistemlərin məlumatların toplanması və emalının (o cümlədən istifadə, açıqlanma, saxlanılma, ötürülmə və məhv edilmə) müəyyən edilən məqsəd üçün lazım olan səviyyə ilə məhdudlaşmasını təmin edəcək formada hazırlanmasını təmin etmək.

7.4.1 Məlumatların toplanmasının məhdudlaşdırılması

Nəzarət tədbiri

Təşkilat FEM-in toplanılmasını müəyyən edilən məqsədlər üçün müvafiq, proporsional və zəruri olan minimum səviyyə ilə məhdudlaşdırmalıdır.

İcra göstərişləri

Təşkilat FEM-in toplanılmasını müəyyən edilən məqsədlər ilə bağlı adekvat, uyğun və zəruri olan səviyyə ilə məhdudlaşdırmalıdır. Buna təşkilatın dolayı şəkildə topladığı FEM-in miqdarının məhdudlaşdırılması daxildir (məs., veb-saytda mövcud qeydlər, sistem qeydləri və s. vasitəsilə).

Standart parametrlərə görə şəxsi həyatın toxunulmazlığı FEM-in toplanılması və emalı zamanı hər hansı seçim imkanı olduğu halda, hər bir seçimin standart parametrlərə görə sıradan çıxarılmalı və yalnız FEM-in subyektinin açıq seçimi ilə aktivləşdirilməli olduğunu ifadə edir.

7.4.2 Məlumatların emalının məhdudlaşdırılması

Nəzarət tədbiri

Təşkilat FEM-in emalını müəyyən edilən məqsədlər üçün adekvat, müvafiq və zəruri olan səviyyə ilə məhdudlaşdırmalıdır.

İcra göstərişləri

FEM-in emalının məhdudlaşdırılması informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı siyasətləri (baxın: 6.2) və onların qəbulu və onlara əməl edilməsi üçün sənədləşdirilmiş prosedurlar vasitəsilə idarə edilməlidir. FEM-in emalı, o cümlədən:

— açıqlanması;

— FEM-in saxlanılma müddəti; və

— kimlərin öz FEM-nə çıxış imkanının olması;

standart parametrlərə görə müəyyən edilən məqsədlərə uyğun olaraq, lazım olan minimum səviyyə ilə məhdudlaşdırılmalıdır.

7.4.3 Dəqiqlik və keyfiyyət

Nəzarət tədbiri

Təşkilat FEM-in emal edilmə dövrü boyunca FEM-in emal edildiyi məqsədlər üçün lazım olduğu qədər dəqiq, tam və müasir olmasını təmin etməli və sənədləşdirməlidir.

İcra göstərişləri

Təşkilat emal etdiyi FEM-də qeyri-dəqiqlik hallarını mümkün qədər azaltmaq üçün siyasətlər, prosedurlar və/və ya mexanizmlər tətbiq etməlidir. Həmçinin qeyri-dəqiq FEM hallarına cavab verməк üçün siyasətlər, prosedurlar və /və ya mexanizmlər də olmalıdır. Bu siyasətlər, prosedurlar və /və ya mexanizmlər sənədləşdirilmiş informasiyaya daxil edilməli (məs., texniki sistem konfiqurasiyaları və s. vasitəsilə) və FEM-in emal dövrü boyunca tətbiq edilməlidir.

Əlavə məlumatlar

FEM-in emal dövrü barədə ətraflı məlumat üçün baxın: ISO/IEC 29101:2018, 6.2.

7.4.4 FEM-in azaldılması məqsədləri

Nəzarət tədbiri

Təşkilat məlumatların azaldılması məqsədlərini və həmin məqsədlərə çatmaq üçün hansı mexanizmlərin (məs., adsızlaşdırılma) istifadə olunmasını müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Təşkilatlar toplanılan və emal edilən xüsusi FEM-in və FEM miqdarının müəyyən edilən məqsədlərə uyğun olaraq necə məhdudlaşdırıldığını müəyyən etməlidir. Buna adsızlaşdırma və ya məlumatların minimuma endirilməsi üzrə digər üsulların istifadəsi daxil ola bilər.

Müəyyən edilən məqsəd (baxın: 7.2.1) adsızlaşdırılmamış FEM-in emalını tələb edə bilər, bu halda təşkilat bu cür emalı təsvir edə bilməlidir.

Digər hallarda müəyyən edilən məqsəd ilkin FEM-in emalını tələb etmir və adsızlaşdırılmış FEM-in emalı müəyyən edilən məqsədə çatmaq üçün kifayət edə bilər. Bu halda təşkilat adsızlaşdırma və/və ya FEM-in minimuma endirilməsi məqsədlərinə çatmaq üçün FEM-in FEM subyekti ilə nə dərəcədə əlaqələndirilməli olduğunu, eləcə də FEM-in emalı üçün nəzərdə tutulan mexanizmləri və üsulları müəyyənləşdirməli və sənədləşdirməlidir.

FEM-i azaltmaq üçün istifadə edilən mexanizmlər emalın növündən və emal üçün istifadə edilən sistemlərdən asılı olaraq dəyişir. Təşkilat məlumatların azaldılması üçün istifadə olunan istənilən mexanizmi (məs., texniki sistem konfiqurasiyaları və s.) sənədləşdirməlidir.

Adsızlaşdırılan məlumatların məqsədlər üçün kifayət etdiyi hallarda təşkilat özünün təyin etdiyi adsızlaşdırma məqsədlərini vaxtında icra etmək üçün nəzərdə tutulan istənilən mexanizmi (məs., texniki sistem konfiqurasiyaları və s.) sənədləşdirməlidir. Məsələn, FEM subyektləri ilə əlaqəli olan xüsusiyyətlərin silinməsi təşkilatın müəyyən edilən məqsədə çatmağına imkan verməkk üçün kifayət edə bilər. Digər hallarda ümumiləşdirmə (məs., yuvarlaqlaşdırma) və ya randomizasiya üsulları (məs., əlavə elementlərin daxil edilməsi) kimi digər adsızlaşdırma üsulları adsızlaşdırılmanın adekvat səviyyəsinə çatmaq üçün istifadə edilə bilər.

QEYD 1 Adsızlaşdırma üsulları barədə ətraflı məlumat üçün baxın: ISO/IEC 20889.

QEYD 2: ISO/IEC 19944 standartı bulud texnologiyaları ilə hesablama ilə əlaqədar məlumatların FEM-in subyektini müəyyən etmə və ya FEM-in subyektini FEM-dəki bir sıra xüsusiyyətlərlə əlaqələndirmə dərəcəsini təsnif etmək üçün istifadə edilə biləcək məlumatların identifikasiyası üzrə təyinedici göstəricilərin tərifini verir.

7.4.5 Emalın sonunda FEM-in adsızlaşdırılması və silinməsi

Nəzarət tədbiri

Təşkilat ilkin FEM müəyyən edilən məqsəd (məqsədlər) üçün artıq lazım olmayanda, FEM-i silməli və ya FEM subyektlərinin identifikasiyasına və ya yenidən identifikasiyasına imkan verməyəcək formaya çevirməlidir.

İcra göstərişləri

Təşkilat artıq əlavə bir emal prosesi gözlənilmədikdə FEM-i silmək üçün mexanizmlərə sahib olmalıdır. Alternativ olaraq, əldə edilən adsızlaşdırılan məlumatlar FEM subyektlərinin yenidən identifikasiyasına ağlabatan formada icazə verə bilmədiyi halda bəzi adsızlaşdırma üsulları istifadə edilə bilər.

7.4.6 Müvəqqəti fayllar

Nəzarət tədbiri

Təşkilat FEM-in emalının nəticəsində yaradılan müvəqqəti faylların müəyyənləşdirilən, sənədləşdirilən müddət çərçivəsində sənədləşdirilmiş prosedurlara uyğun olaraq silinməsini (məs., silinməsini və ya məhv edilməsini) təmin etməlidir.

İcra göstərişləri

Təşkilat istifadə edilməyən müvəqqəti faylların müəyyənləşdirilən müddətdə silindiyinə dair vaxtaşırı yoxlamalar həyata keçirməlidir.

Digər məlumatlar

İnformasiya sistemləri normal fəaliyyətləri dövründə müvəqqəti fayllar yarada bilər. Bu cür fayllar sistem və ya tətbiq üçün xarakterikdir, lakin onlara məlumat bazalarının yenilənməsi və digər proqram təminatının işləməsi ilə əlaqədar fayl sisteminin əvvəlki versiyasının bərpa edilməsi qeydləri və müvəqqəti fayllar daxil ola bilər. Müvəqqəti fayllara müvafiq məlumatların emalı tapşırığı tamamlandıqdan sonra ehtiyac olmur, lakin onların silinə bilmədiyi hallar mövcuddur. Bu faylların istifadə edilmə müddəti hər zaman müəyyən olmur, lakin "lazımsız faylları silmə" proseduru müvafiq faylları müəyyənləşdirməli və onların ən son istifadə edildiyi vaxtdan nə qədər keçdiyini müəyyən etməlidir.

7.4.7 Məlumatların saxlanması

Nəzarət tədbiri

Təşkilat FEM-i emal edildiyi məqsədlər üçün lazım olan müddətdən daha uzun müddət ərzində saxlamamalıdır.

İcra göstərişləri

Təşkilat FEM-in lazım olduğundan daha uzun müddət saxlanılmama tələbini nəzərə alaraq, saxladığı məlumatlar üçün saxlanılma planı hazırlamalı və onu həyata keçirməlidir. Bu cür planlar hüquqi, normativ və iş tələblərini nəzərə almalıdır. Bu cür tələblərin bir-birinə zidd olduğu halda, işgüzar qərarlar alınmalı (risklərin qiymətləndirilməsi əsasında) və müvafiq planda sənədləşdirilməlidir.

7.4.8 Məlumatların məhv edilməsi

Nəzarət tədbiri

Təşkilat FEM-in məhv edilməsi üçün sənədləşdirilən siyasətlərə, prosedurlara və/və ya mexanizmlərə sahib olmalıdır.

İcra göstərişləri

FEM-in məhv edilməsi üsullarının seçilməsi bir sıra amillərdən asılıdır, çünki məlumatların məhv edilmə üsulları öz xüsusiyyətlərinə və nəticələrinə görə fərqlənir (məsələn, əldə olunan maddi daşıyıcının dəqiqlik dərəcəsi və ya elektron daşıyıcıda silinən məlumatların geri qaytarıla bilməsi). Müvafiq məhv edilmə üsulu seçilərkən nəzərə alınmalı amillərə məhv ediləcək FEM-in xarakteri və həcmi, FEM ilə əlaqəli metaməlumatların olub-olmaması və FEM-in saxlanıldığı daşıyıcının fiziki xüsusiyyətləri daxildir, lakin bu amillər sadalananlarla məhdudlaşmır.

7.4.9 FEM-in ötürülməsinə nəzarət tədbirləri

Nəzarət tədbiri

Təşkilat məlumatların ötürülməsi şəbəkəsi ilə ötürülən FEM-i (məs., başqa bir təşkilata göndərilən) məlumatların nəzərdə tutulan təyinat nöqtəsinə çatmasını təmin etmək üçün hazırlanan müvafiq nəzarət tədbirlərinə cəlb etməlidir.

İcra göstərişləri

Adətən təkcə müvafiq icazəyə malik fərdlərin ötürmə sistemlərinə çıxış imkanının olmasını təmin etməklə və FEM-in düzgün resipiyentlərə təhlükəsiz şəkildə ötürülməsini təmin etmək üçün müvafiq prosesləri yerinə yetirməklə (o cümlədən audit qeydlərinin saxlanması) FEM-in ötürülməsinə nəzarət edilməlidir.

7.5 FEM-in paylaşılması, ötürülməsi və açıqlanması

Məqsəd: FEM-in paylaşılıb-paylaşılmadığını, başqa yurisdiksiyalara və ya üçüncü tərəflərə ötürülüb-ötürülmədiyini və/və ya müvafiq öhdəliklərə uyğun olaraq açıqlanıb-açıqlanmadığını müəyyənləşdirmək və sənədləşdirmək.

7.5.1 FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsasın müəyyən edilməsi

Nəzarət tədbiri

Təşkilat FEM-in yurisdiksiyalar arasında ötürülməsi üçün müvafiq əsası müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

FEM-in ötürülməsi məlumatların ötürüləcəyi yurisdiksiyadan və ya beynəlxalq təşkilatdan (və haradan əldə edildiyindən) asılı olaraq, qanunvericilik və/və ya normativ aktlarla tənzimlənə bilər. Təşkilat ötürülmənin əsası olaraq bu cür tələblərə uyğunluğu sənədləşdirməlidir.

Bəzi yurisdiksiyalar məlumatların ötürülməsi müqavilələrinin müəyyən edilən nəzarət orqanı tərəfindən nəzərdən keçirilməsini tələb edə bilər. Bu cür yurisdiksiyalar çərçivəsində fəaliyyət göstərən təşkilatlar bu cür hər hansı tələblərdən xəbərdar olmalıdır.

QEYD: Ötürülmə əməliyyatları müəyyən bir yurisdiksiya daxilində həyata keçirilərkən, tətbiq olunan qanunvericilik və/ və ya normativ aktlar göndərən və resipiyent üçün eyni olur.

7.5.2 FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar

Nəzarət tədbiri

Təşkilat FEM-in ötürülə biləcəyi ölkələri və beynəlxalq təşkilatları dəqiqliklə müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Normal əməliyyatlarda FEM-in ötürülə biləcəyi ölkələrin və beynəlxalq təşkilatların adları müştərilər üçün əlçatan olmalıdır. Subpodrat əsaslı müqaviləyə cəlb olunmuş FEM-in emalından istifadə etməkdən əldə edilən ölkələrin adları daxil edilməlidir. Daxil edilən ölkələr 7.5.1 ilə əlaqədar nəzərdən keçirilməlidir.

Normal əməliyyatlardan kənarda hüquq-mühafizə orqanının tələbi ilə həyata keçirilən, ölkələrin adlarının əvvəlcədən tam müəyyənləşdirilə bilmədiyi və ya hüquq-mühafizə araşdırmasının məxfiliyini qorumaq üçün tətbiq olunan yurisdiksiyaların qadağan etdiyi ötürmə halları ola bilər (baxın: 7.5.1, 8.5.4 və 8.5.5).

7.5.3 FEM-in ötürülməsinə dair qeydlər

Nəzarət tədbiri

Təşkilat FEM-in üçüncü tərəflərə və ya üçüncü tərəflərdən ötürülmə əməliyyatlarını qeyd etməli və FEM subyektləri qarşısında olan öhdəlikləri ilə bağlı gələcək müraciətləri dəstəkləmək üçün bu tərəflərlə əməkdaşlığı təmin etməlidir.

İcra göstərişləri

Qeydlərə FEM nəzarətçilərinin öz öhdəliklərini yerinə yetirməyinin nəticəsi olaraq dəyişdirilmiş FEM-in üçüncü tərəflərdən ötürülmə əməliyyatları və ya FEM subyektlərinin qanuni tələblərini, o cümlədən FEM-i silmək tələblərini (məs., razılığın geri götürülməsindən sonra) icra etmək üçün FEM-in üçüncü tərəflərə ötürülməsi əməliyyatları daxil ola bilər.

Təşkilat bu qeydlərin saxlanılma müddətini müəyyən edən siyasətə sahib olmalıdır.

Təşkilat yalnız qəti şəkildə lazım olan məlumatları saxlamaqla məlumatların azaldılması prinsipini ötürülmə barədə qeydlərə tətbiq etməlidir.

7.5.4 FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər

Nəzarət tədbiri

Təşkilat FEM-in üçüncü tərəflərə açıqlanmasını, o cümlədən hansı FEM-in açıqlandığını, kimə və nə vaxt açıqlandığını qeyd etməlidir.

İcra göstərişləri

FEM normal əməliyyatlar vaxtı açıqlana bilər. Bu açıqlama əməliyyatları qeydə alınmalıdır. Qanuni araşdırmalar və ya xarici auditlərdən irəli gələn açıqlamalar kimi üçüncü tərəflərə edilən əlavə açıqlamalar da qeyd edilməlidir. Qeydlərə açıqlanan məlumatların mənbəyi və açıqlama səlahiyyətinin mənbəyi daxil edilməlidir.

8 FEM-i emal edən tərəflər üçün ISO/IEC 27002 üzrə əlavə göstərişlər

8.1 Ümumi müddəalar

Maddə 6-da göstərişlər və bu maddədəki əlavələr FEM-i emal edən tərəflər üçün FMİS-ə aid göstərişləri formalaşdırır. Bu maddədəki sənədləşdirilən icra göstərişləri Qoşma B-də sadalanan nəzarət tədbirləri ilə bağlıdır.

8.2 Məlumatların toplanması və emalı şərtləri

Məqsəd: Emal prosesinin qanuni olduğunu, tətbiq olunan yurisdiksiyalara görə hüquqi əsasının olduğunu və aydın şəkildə müəyyənləşdirilən və qanuni məqsədləri olduğunu müəyyənləşdirmək və sənədləşdirmək.

8.2.1 Müştəri ilə müqavilə

Nəzarət tədbiri

Təşkilat müvafiq halda FEM-in emalı ilə bağlı müqavilənin müştərinin öhdəliklərinə yardımın təmin edilməsində təşkilatın rolunu nəzərə almasını təmin etməlidir (emalın xarakterini və təşkilat üçün əlçatan olan məlumatları nəzərə alaraq).

İcra göstərişləri

Təşkilat ilə müştəri arasında bağlanan müqavilə müvafiq halda və müştərinin rolundan (FEM nəzarətçisi və ya FEM-i emal edən tərəf) asılı olaraq, aşağıdakıları ehtiva etməlidir (bu siyahı nə tam, nə də müfəssəl deyil):

— layihəyə və standart parametrlərə görə şəxsi həyatın toxunulmazlığı (baxın: 7.4, 8.4);

— emal prosesinin təhlükəsizliyinin təmin olunması;

— FEM-i ehtiva edən pozuntuların nəzarət orqanına bildirilməsi;

— FEM-i ehtiva edən pozuntuların müştərilərə və FEM subyektlərinə bildirilməsi;

— Şəxsi həyatın toxunulmazlığına Təsirin Qiymətləndirilməsinin aparılması; və

— FEM-in mühafizəsi üzrə müvafiq orqanlarla əvvəlcədən məsləhətləşmələrə ehtiyac olarsa, FEM-i emal edən tərəf tərəfindən yardımın təmin edilməsi.

Bəzi yurisdiksiyalar müqavilənin emal mövzusunu və müddətini, emalın xarakterini və məqsədini, FEM-in növünü və FEM subyektlərinin kateqoriyalarını ehtiva etməyini tələb edir.

8.2.2 Təşkilatın məqsədləri

Nəzarət tədbiri

Təşkilat müştəri adından emal edilən FEM-in yalnız müştərinin sənədləşdirilmiş təlimatlarında göstərilən məqsədlər üçün emal edilməsini təmin etməlidir.

İcra göstərişləri

Təşkilat ilə müştəri arasında bağlanan müqavilə xidmətlə nail olunacaq məqsədi və vaxt çərçivəsini ehtiva etməlidir, lakin bununla məhdudlaşmamalıdır.

Müştərinin məqsədinə nail olmaq üçün müştərinin ümumi təlimatlarına uyğun olaraq, lakin müştərinin aydın təlimatı olmadan təşkilatın FEM-in emalı metodunu müəyyənləşdirməsinin uyğunluğunun texniki səbəbləri ola bilər. Məsələn, şəbəkədən və ya emal imkanından səmərəli şəkildə istifadə etmək üçün FEM-in subyektinin müəyyən xüsusiyyətlərindən asılı olaraq, xüsusi emal resurslarını bölüşdürmək zəruri ola bilər.

Təşkilat müştərinin məqsədin aydınlaşdırılması və məhdudlaşdırma prinsiplərinə əməl etməyini təsdiqləməsinə icazə verməlidir. Bu, heç bir FEM-in təşkilat və ya onun hər hansı subpodratçısı tərəfindən müştərinin sənədləşdirilmiş təlimatlarında göstərilən məqsədlərdən başqa məqsədlər üçün emal edilməməsini də təmin edir.

8.2.3 Marketinq və reklam məqsədilə istifadə

Nəzarət tədbiri

Təşkilat FEM-in müvafiq subyektindən əvvəlcədən razılıq alındığını müəyyənləşdirmədən müqavilə çərçivəsində emal edilən FEM-i marketinq və reklam məqsədi ilə istifadə etməməlidir. Təşkilat bu cür razılığı verməyi xidmətin alınması üçün şərtə çevirməməlidir.

İcra göstərişləri

FEM-i emal edən tərəflərin müştərinin müqavilə əsaslı tələblərinə əməl etməsi xüsusilə marketinqin və/və ya reklamın planlaşdırıldığı halda sənədləşdirilməlidir.

Təşkilatlar FEM subyektlərindən ədalətli formada aydın razılıq alınmadığı halda marketinq və/və ya reklam məqsədilə istifadənin daxil edilməsini təkid etməməlidir.

QEYD: Bu nəzarət tədbiri 8.2.2 bəndindəki daha ümumi nəzarət tədbirinə əlavədir və onu əvəz etmir və ya başqa şəkildə ondan daha üstün deyil.

8.2.4 Pozuntuya yol verən təlimat

Nəzarət tədbiri

Təşkilat emal təlimatının tətbiq olunan qanunvericiliyi və/və ya normativ aktları pozduğunu düşünürsə, müştərini məlumatlandırmalıdır.

İcra göstərişləri

Təşkilatın təlimatın tətbiq olunan qanunvericiliyi və/və ya normativ aktları pozub-pozmadığını təsdiqləmə qabiliyyəti texnoloji kontekstdən, təlimatın özündən və təşkilat ilə müştəri arasında bağlanan müqavilədən asılı ola bilər.

8.2.5 Müştərinin öhdəlikləri

Nəzarət tədbiri

Təşkilat müştərini müvafiq məlumatlarla təmin etməlidir ki, müştəri öz öhdəliklərinə əməl etdiyini göstərə bilsin.

İcra göstərişləri

Müştəriyə lazım olan məlumatlara təşkilatın müştəri və ya müştərinin səlahiyyət verdiyi, yaxud başqa formada razılaşdırılan başqa auditor tərəfindən audit aparılmasına icazə verib-verməməsi və ona töhfə verib-verməməsi daxil ola bilər.

8.2.6 FEM-in emalı ilə əlaqəli qeydlər

Nəzarət tədbiri

Təşkilat müştəri adına həyata keçirilən FEM-in emalı üçün öz öhdəliklərinə (müvafiq müqavilədə müəyyənləşdirildiyi kimi) əməl etməyini nümayiş etdirmək məqsədilə lazımi qeydləri müəyyənləşdirməli və saxlamalıdır.

İcra göstərişləri

Bəzi yurisdiksiyalar təşkilatın aşağıdakı məlumatları qeydə almağını tələb edə bilər:

— hər bir müştərinin adına həyata keçirilən emal prosesinin kateqoriyaları;

— məlumatların üçüncü ölkələrə və ya beynəlxalq təşkilatlara ötürülməsi əməliyyatları; və

— texniki və təşkilati təhlükəsizlik tədbirlərinin ümumi təsviri.

8.3 FEM subyektləri qarşısında öhdəliklər

Məqsəd: FEM subyektlərinə özlərinin FEM-nin emalı barədə müvafiq məlumatların verilməsini təmin etmək və FEM subyektləri qarşısında FEM-in emalı ilə bağlı hər hansı digər müvafiq öhdəlikləri yerinə yetirmək.

8.3.1 FEM subyektləri qarşısında öhdəliklər

Nəzarət tədbiri

Təşkilat müştərini FEM subyektləri ilə bağlı öhdəliklərinə əməl etmək üçün vasitələrlə təmin etməlidir.

İcra göstərişləri

FEM nəzarətçisinin öhdəlikləri qanunvericilik, hüquqi sənədlər və/və ya müqavilə ilə müəyyənləşdirilə bilər. Bu öhdəliklərə müştərinin həmin öhdəlikləri həyata keçirmək üçün təşkilatın xidmətlərindən istifadə etdiyi məsələlər daxil ola bilər. Məsələn, buna FEM-ə vaxtında düzəliş edilməsi və ya silinməsi daxil ola bilər.

Müştəri FEM subyektləri qarşısında öhdəliklərini yerinə yetirməyi asanlaşdıracaq məlumatlar və ya texniki tədbirlər üçün təşkilatdan asılı olduğu halda müvafiq məlumatlar və ya texniki tədbirlər müqavilədə dəqiqliklə müəyyənləşdirilməlidir.

8.4 Layihəyə görə və standart parametrlərə görə şəxsi həyatın toxunulmazlığı

Məqsəd: Proseslərin və sistemlərin FEM-in toplanması və emalının (o cümlədən istifadə, açıqlanma, saxlanılma, ötürülmə və məhv edilmə) müəyyən edilən məqsəd üçün lazım olan səviyyə ilə məhdudlaşmasını təmin edəcək formada hazırlanmasını təmin etmək.

8.4.1 Müvəqqəti fayllar

Nəzarət tədbiri

Təşkilat FEM-in emalının nəticəsində yaradılan müvəqqəti faylların müəyyənləşdirilən, sənədləşdirilən müddət çərçivəsində sənədləşdirilmiş prosedurlara uyğun olaraq silinməsini (məs., silinməsini və ya məhv edilməsini) təmin etməlidir.

İcra göstərişləri

Təşkilat istifadə edilməyən müvəqqəti faylların müəyyənləşdirilən müddətdə silindiyinə dair vaxtaşırı yoxlama aparmalıdır.

Digər məlumatlar

İnformasiya sistemləri normal fəaliyyətləri dövründə müvəqqəti fayllar yarada bilər. Bu cür fayllar sistem və ya tətbiq üçün xarakterikdir, lakin onlara məlumat bazalarının yenilənməsi və digər proqram təminatının işləməsi ilə əlaqədar fayl sisteminin əvvəlki versiyasının bərpa edilməsi qeydləri və müvəqqəti fayllar daxil ola bilər. Müvəqqəti fayllara müvafiq məlumatların emalı tapşırığı tamamlandıqdan sonra ehtiyac olmur, lakin onların silinə bilmədiyi hallar mövcuddur. Bu faylların istifadə edilmə müddəti hər zaman müəyyən olmur, lakin "lazımsız faylları silmə" proseduru müvafiq faylları müəyyənləşdirməli və onların ən son istifadə edildiyi vaxtdan nə qədər keçdiyini müəyyən etməlidir.

8.4.2 FEM-in qaytarılması, ötürülməsi və ya məhv edilməsi

Nəzarət tədbiri

Təşkilat FEM-in təhlükəsiz şəkildə qaytarıla, ötürülə və/və ya məhv edilə bilməsini təmin etməlidir. Bu, onun siyasətini müştəri üçün də əlçatan etməlidir.

İcra göstərişləri

Müəyyən bir anda FEM-in hər hansı şəkildə silinməsinə ehtiyac ola bilər. O, FEM-in müştəriyə qaytarılmasını, onun başqa təşkilata və ya FEM nəzarətçisinə ötürülməsini (məs., birləşmə nəticəsində), silinməsini və ya başqa formada məhv edilməsini, adsızlaşdırılmasını və ya arxivləşdirilməsini ehtiva edə bilər. FEM-in geri qaytarılma, ötürülmə və/və ya məhv edilmə imkanı təhlükəsiz qaydada idarə edilməlidir.

Təşkilat müştərinin müqavilə çərçivəsində emal edilən FEM-in onun müəyyənləşdirilən məqsədləri, o cümlədən ehtiyat nüsxənin çıxarılması və işin davamlılığı məqsədləri üçün artıq lazım olmadığı halda saxlandığı yerdən silinməsini (təşkilat və ya onun hər hansı subpodratçısı tərəfindən) təmin etməsinə imkan vermək üçün lazımi təminatı verməlidir.

Təşkilat FEM-in məhv edilməsi ilə bağlı siyasəti hazırlamalı və onu icra etməli və tələb olunduğu halda bu siyasəti müştəriyə təqdim etməlidir.

Siyasət müqavilənin təsadüfi pozulması nəticəsində müştərini öz FEM-ni itirməkdən qorumaq üçün müqavilə bitdikdən sonra FEM məhv edilməzdən əvvəl onun saxlanılma müddətini əhatə etməlidir.

QEYD: Bu nəzarət tədbiri və göstərişlər məlumatların saxlanması prinsipi çərçivəsində də tətbiq olunur (baxın:7.4.7).

8.4.3 FEM-in ötürülməsinə nəzarət tədbirləri

Nəzarət tədbiri

Təşkilat məlumatların ötürülməsi şəbəkəsi ilə ötürülən FEM-i məlumatların nəzərdə tutulan təyinat nöqtəsinə çatmasını təmin etmək üçün hazırlanan müvafiq nəzarət tədbirlərinə müvafiq şəkildə ötürməlidir.

İcra göstərişləri

Adətən yalnız müvafiq icazəyə malik fərdlərin ötürmə sistemlərinə çıxış imkanının olmasını təmin etməklə və FEM-in düzgün resipiyentlərə təhlükəsiz şəkildə ötürülməsini təmin etmək üçün lazımi

prosesləri yerinə yetirməklə (o cümlədən audit məlumatlarının saxlanması) FEM-in ötürülməsinə nəzarət edilməlidir. Ötürməyə nəzarət tədbirləri üzrə tələblər FEM-i emal edən tərəflə müştəri arasında bağlanan müqaviləyə daxil edilə bilər.

Ötürmə ilə bağlı heç bir müqavilə əsaslı tələblər olmadığı halda ötürülmədən əvvəl müştəridən məsləhət alınması münasib ola bilər.

8.5 FEM-in paylaşılması, ötürülməsi və açıqlanması

Məqsəd: FEM-in paylaşılıb-paylaşılmadığını, başqa yurisdiksiyalara və ya üçüncü tərəflərə ötürülüb-ötürülmədiyini və/və ya müvafiq öhdəliklərə uyğun olaraq açıqlanıb-açıqlanmadığını müəyyənləşdirmək və sənədləşdirmək.

8.5.1 FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsas

Nəzarət tədbiri

Təşkilat müştərini FEM-in yurisdiksiyalar arasında ötürülməsi əməliyyatlarının əsası və bu baxımdan edilməsi nəzərdə tutulan hər hansı dəyişikliklər barədə vaxtında məlumatlandırmalıdır ki, müştəri bu cür dəyişikliklərə etiraz edə və ya müqaviləyə xitam verə bilsin.

İcra göstərişləri

FEM-in yurisdiksiyalar arasında ötürülməsi FEM-in ötürüləcəyi yurisdiksiya və ya təşkilatdan (və haradan əldə edildiyindən) asılı olaraq, qanunvericilik və/və ya normativ aktlarla tənzimlənə bilər. Təşkilat ötürmənin əsası olaraq bu cür tələblərə əməl edildiyini sənədləşdirməlidir.

Təşkilat FEM-in hər hansı ötürülməsi halı, o cümlədən aşağıdakılara ötürülməsi barədə müştəriyə məlumat verməlidir:

— təchizatçılar;

— digər tərəflər;

— digər ölkələr və ya beynəlxalq təşkilatlar.

Dəyişikliklər edildiyi zaman təşkilat müştəriyə razılaşdırılmış vaxt çərçivəsinə əsasən əvvəlcədən məlumat verməlidir ki, müştəri bu cür dəyişikliklərə etiraz edə və ya müqaviləyə xitam verə bilsin.

Təşkilat ilə müştəri arasında bağlanan müqavilədə təşkilatın müştəriyə xəbər vermədən dəyişikliklər edə biləcəyi maddələr ola bilər. Belə hallarda bu güzəştin sərhədləri təyin edilməlidir (məs., təşkilat müştəriyə xəbər vermədən təchizatçıları dəyişə bilər, lakin FEM-i başqa ölkələrə ötürə bilməz).

FEM-in beynəlxalq səviyyədə ötürülməsi zamanı müqavilələr (məs., Standart Müqavilə maddələri", "Hüquqi öhdəlik yaradan Korporativ Qaydalar" və ya "Sərhədlərarası Şəxsi həyatın toxunulmazlığı Qaydaları"), müvafiq ölkələr və bu cür müqavilələrin tətbiq edildiyi hallar müəyyənləşdirilməlidir.

8.5.2 FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar

Nəzarət tədbiri

Təşkilat FEM-in ötürülə biləcəyi ölkələri və beynəlxalq təşkilatları dəqiqliklə müəyyənləşdirməli və sənədləşdirməlidir.

İcra göstərişləri

Normal əməliyyatlarda FEM-in ötürülə biləcəyi ölkələrin və beynəlxalq təşkilatların adları müştərilər üçün əlçatan olmalıdır. Subpodrat əsaslı müqaviləyə cəlb olunmuş FEM-in emalından istifadə etməkdən əldə edilən ölkələrin adları daxil edilməlidir. Daxil edilən ölkələr 8.5.1 ilə əlaqəli olaraq nəzərə alınmalıdır.

Normal əməliyyatlardan kənarda hüquq-mühafizə orqanının tələbi ilə həyata keçirilən, ölkələrin adlarının əvvəlcədən tam müəyyənləşdirilə bilmədiyi və ya hüquq-mühafizə araşdırmasının məxfiliyini qorumaq üçün tətbiq olunan yurisdiksiyaların qadağan etdiyi ötürmə halları ola bilər (baxın: 7.5.1, 8.5.4 və 8.5.5).

8.5.3 FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər

Nəzarət tədbiri

Təşkilat FEM-in üçüncü tərəflərə açıqlanması hallarını, o cümlədən hansı FEM-in açıqlandığını, kimə və nə vaxt açıqlandığını qeyd etməlidir.

İcra göstərişləri

FEM normal əməliyyatlar vaxtı açıqlana bilər. Bu açıqlama əməliyyatları qeydə alınmalıdır. Qanuni araşdırmalar və ya xarici auditlərdən irəli gələn açıqlamalar kimi üçüncü tərəflərə edilən əlavə açıqlamalar da qeyd edilməlidir. Qeydlərə açıqlanan məlumatların mənbəyi və açıqlama səlahiyyətinin mənbəyi daxil edilməlidir.

8.5.4 FEM-in açıqlanması ilə bağlı sorğuların bildirilməsi

Nəzarət tədbiri

Təşkilat FEM-in açıqlanması üçün hüquqi öhdəlik yaradan hər hansı müraciətləri müştəriyə bildirməlidir.

İcra göstərişləri

Təşkilat FEM-in açıqlanmasına dair hüquqi öhdəlik yaradan müraciətlər ala bilər (məs., hüquq-mühafizə orqanlarından). Belə hallarda təşkilat bu cür hər hansı müraciəti razılaşdırılan müddət çərçivəsində və razılaşdırılan prosedura (müştəri müqaviləsinə daxil edilə bilən) əsasən müştəriyə bildirməlidir.

Bəzi hallarda hüquqi öhdəlik yaradan müraciətlərə təşkilatın hadisə barədə heç kimə xəbər verməməsi tələbi daxildir (məlumatların açıqlanmasına mümkün qadağaya nümunə kimi cinayət hüququ çərçivəsində hüquq-mühafizə araşdırmasının məxfiliyinin qorunması qadağasını göstərmək olar).

8.5.5 FEM-in açıqlanmasının hüquqi öhdəlik yaratdığı hallar

Nəzarət tədbiri

Təşkilat FEM-in hüquqi öhdəlik yaratmayan açıqlanma hallarına dair hər hansı müraciətlərdən imtina etməli, hər hansı FEM-i açıqlamazdan əvvəl müvafiq müştəri ilə məsləhətləşməli və müvafiq müştərinin icazə verdiyi FEM-in açıqlanması üçün müqavilə ilə razılaşdırılan tələbləri qəbul etməlidir.

İcra göstərişləri

Nəzarət tədbirinin icrası ilə bağlı təfərrüatlar müştəri müqaviləsinə daxil edilə bilər.

Bu cür müraciətlər bir sıra mənbələrdən, o cümlədən məhkəmələrdən, tribunallardan və inzibati orqanlardan gələ bilər. Onlar hər hansı yurisdiksiyadan qaynaqlana bilər.

8.5.6 FEM-in emalı üçün istifadə edilən subpodratçıların açıqlanması

Nəzarət tədbiri

Təşkilat FEM-in emalı üçün hər hansı subpodratçılardan istifadə etməzdən əvvəl subpodratçıdan istifadə barədə müştəriyə xəbər verməlidir.

İcra göstərişləri

FEM-in emalı üçün subpodratçılardan istifadəyə dair müddəalar müştəri ilə müqaviləyə daxil edilməlidir.

Açıqlanan məlumatlar subpodratçıdan istifadə edilməsi faktını və müvafiq subpodratçıların adlarını əhatə etməlidir. Açıqlanan məlumatlar subpodratçıların məlumatları ötürə biləcəyi ölkələri və beynəlxalq təşkilatları (baxın: 8.5.2) və subpodratçıların təşkilatın öhdəliklərini yerinə yetirməli və ya qarşılamalı olduğu vasitələri (baxın: 8.5.7) də ehtiva etməlidir.

Subpodratçı məlumatlarının ictimaiyyətə açıqlanması təhlükəsizlik riskini məqbul həddən yüksək səviyyədə artırdığı hallarda məlumatların açıqlanması məlumatların açıqlanmamasına dair müqavilələr çərçivəsində və/və ya müştərinin sorğusu əsasında həyata keçirilməlidir. Müştəri məlumatların əlçatan olması barədə məlumatlandırılmalıdır.

Bu, FEM-in ötürülə biləcəyi ölkələrin siyahısına şamil edilmir. Bu siyahı istənilən halda müştərilərə müvafiq FEM subyektlərini məlumatlandırmağa icazə verəcək qaydada açıqlanmalıdır.

8.5.7 FEM-in emalı üçün subpodratçının cəlb edilməsi

Nəzarət tədbiri

Təşkilat FEM-in emalı üçün subpodratçını yalnız müştəri müqaviləsinə əsasən cəlb etməlidir.

İcra göstərişləri

Təşkilat həmin FEM-in emalının bir hissəsi və ya hamısını başqa bir təşkilata həvalə etdiyi halda müştərinin yazılı icazəsi FEM-in subpodratçı tərəfindən emalından əvvəl tələb olunur. Bu, müştəri ilə müqavilədə müvafiq maddələr formasında, yaxud xüsusi birdəfəlik müqavilə ola bilər.

Təşkilat öz adından FEM-in emalı üçün istifadə etdiyi hər hansı subpodratçılarla yazılı müqavilə bağlamalı və subpodratçılarla müqavilələrinin Qoşma B-dəki müvafiq nəzarət tədbirlərinin icrasını əhatə etməsinə əmin olmalıdır.

Təşkilat ilə onun adından FEM-in emalını həyata keçirən hər hansı subpodratçı arasında bağlanan müqavilə subpodratçının informasiya təhlükəsizliyinə yönəlmiş risklərin qiymətləndirilməsi prosesini (baxın: 5.4.1.2) və FEM-i emal edən tərəfin həyata keçirdiyi FEM-in emalı prosesinin əhatə dairəsini (baxın: 6.12) nəzərə alaraq, Qoşma B-də müəyyənləşdirilən müvafiq nəzarət tədbirlərini icra etməsini tələb etməlidir. Standart olaraq, Qoşma B-də müəyyənləşdirilən bütün nəzarət tədbirlərinin münasib olduğu qəbul edilməlidir. Təşkilat subpodratçının Qoşma B-dəki nəzarət tədbirini icra etməsini tələb etməməyə qərar verirsə, həmin nəzarət tədbirinin istisna edilməsini əsaslandırmalıdır.

Müqavilə hər bir tərəfin məsuliyyətlərini fərqli şəkildə müəyyənləşdirə bilər, lakin bu sənədə uyğun olmaq üçün bütün nəzarət tədbirləri nəzərə alınmalı və sənədləşdirilmiş informasiyaya daxil edilməlidir.

8.5.8 FEM-in emalı üçün subpodratçının dəyişdirilməsi

Nəzarət tədbiri

Ümumi yazılı icazə olduğu halda, təşkilat FEM-in emalı üçün subpodratçıların əlavə edilməsi və ya dəyişdirilməsi ilə bağlı nəzərdə tutulan hər hansı dəyişikliklər barədə müştərini məlumatlandırmalı, bununla müştəriyə bu cür dəyişikliklərə etiraz etmək imkanı verməlidir.

İcra göstərişləri

Təşkilat sözügedən FEM-in emalının bir hissəsini və ya hamısını həvalə etdiyi təşkilatı dəyişdirdiyi halda, FEM yeni subpodratçı tərəfindən emal edilməzdən əvvəl dəyişiklik üçün müştərinin yazılı icazəsi tələb olunur. Bu, müştəri ilə müqavilədə müvafiq maddələr formasında, yaxud xüsusi birdəfəlik müqavilə ola bilər.

Qoşma A
(normativ)

FMİS-ə aid nəzarət məqsədləri və nəzarət tədbirləri (FEM Nəzarətçiləri)

Bu Qoşma FEM-i emal edən tərəflərdən istifadə edən və ya istifadə etməyən FEM nəzarətçiləri kimi çıxış edən təşkilatlar üçün nəzərdə tutulub. O, ISO/IEC 27001:2013 standartındakı Qoşma A-nı daha geniş formatda təqdim edir.

Cədvəl A.1-də sadalanan əlavə və ya dəyişdirilmiş nəzarət məqsədləri və nəzarət tədbirləri birbaşa olaraq bu sənəddə müəyyənləşdirilən nəzarət məqsədlərindən və nəzarət tədbirlərindən irəli gəlir və onlarla uzlaşır və ISO/IEC 27001:2013 standartının 5.4.1.3 bəndində təkmilləşdirilən 6.1.3 bəndi kontekstində istifadə edilməlidir.

Bu Qoşmada sadalanan nəzarət məqsədlərinin və nəzarət tədbirlərinin hamısının FMİS-in icrasına daxil edilməsinə ehtiyac yoxdur. İstisna edilən hər hansı nəzarət məqsədlərinin əsaslandırılması Tətbiq Bəyanatına daxil edilməlidir (baxın:5.4.1.3). İstisna üçün əsaslandırmaya nəzarət tədbirlərinin risklərin qiymətləndirilməsinə görə zəruri hesab edilmədiyi və tətbiq olunan qanunvericilik və/və ya normativ aktların tələb etmədiyi (və ya istisnalara məruz qaldığı) hallar daxil ola bilər.

QEYD: Bu Qoşmadakı maddə nömrələri Maddə 7-dəki bənd nömrələri ilə əlaqəlidir.

Cədvəl A.1 — Nəzarət məqsədləri və nəzarət tədbirləri

A.7.2 Məlumatların toplanması və emalı şərtləri Məqsəd: Emal prosesinin qanuni olduğunu, tətbiq olunan yurisdiksiyalara görə hüquqi əsasının olduğunu və aydın şəkildə müəyyənləşdirilən və qanuni məqsədləri olduğunu müəyyənləşdirmək və sənədləşdirmək.		
A.7.2.1	Məqsədin müəyyənləşdirilməsi və sənədləşdirilməsi	*Nəzarət tədbiri* Təşkilat FEM-in emalı üçün xüsusi məqsədləri müəyyənləşdirməli və sənədləşdirməlidir.
A.7.2.2	Hüquqi əsasın müəyyən edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in müəyyənləşdirilən məqsədlər çərçivəsində emalı üçün müvafiq hüquqi əsası müəyyənləşdirməli, sənədləşdirməli və ona əməl etməlidir.
A.7.2.3	Razılığın nə vaxt və necə alınacağının müəyyən edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in emalı üçün FEM subyektlərindən razılıq alınıb-alınmadığını, nə vaxt və necə alındığını göstərə biləcəyi müəyyən proses müəyyənləşdirməli və sənədləşdirməlidir.
A.7.2.4	Razılığın əldə edilməsi və qeydə alınması	*Nəzarət tədbiri* Təşkilat sənədləşdirilən proseslərə əsasən FEM subyektlərindən razılıq almalı və razılığı qeyd etməlidir.
A.7.2.5	Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi	*Nəzarət tədbiri* Təşkilat FEM-in yeni emal prosesi və ya FEM-in mövcud emal prosesinə dəyişikliklər planlaşdırılarkən şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi ehtiyaclarını qiymətləndirməli və müvafiq olduqda icra etməlidir.
A.7.2.6	FEM-i emal edən tərəflərlə müqavilələr	*Nəzarət tədbiri* Təşkilat istifadə etdiyi hər hansı FEM-i emal edən tərəflə yazılı müqavilə bağlamalı və FEM-i emal edən tərəflərlə müqavilələrinin Qoşma B-dəki müvafiq nəzarət tədbirlərinin icrasını əhatə etməsini təmin etməlidir.

Cədvəl A.1 *(davamı)*

A.7.2.7	Birgə FEM nəzarətçisi	*Nəzarət tədbiri* Təşkilat FEM-in hər hansı birgə FEM nəzarətçisi ilə birgə emalına (o cümlədən FEM-in mühafizəsi və təhlükəsizlik tələbləri) dair müvafiq vəzifə və öhdəlikləri müəyyənləşdirməlidir.
A.7.2.8	FEM-in emalı ilə əlaqəli qeydlər	*Nəzarət tədbiri* Təşkilat FEM-in emalına dair öhdəliklərinin dəstəklənməsi üçün zəruri qeydləri müəyyənləşdirməli və onları təhlükəsiz şəkildə saxlamalıdır.
A.7.3 FEM subyektləri qarşısında öhdəliklər Məqsəd: FEM subyektlərinə onların FEM-nin emalı barədə müvafiq məlumatların verilməsini təmin etmək və FEM subyektləri qarşısında FEM-in emalı ilə bağlı hər hansı digər müvafiq öhdəlikləri qarşılamaq.		
A.7.3.1	FEM subyektləri qarşısında öhdəliklərin müəyyən edilməsi və yerinə yetirilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərinin FEM-nin emalı ilə bağlı onların qarşısında hüquqi, normativ və iş öhdəliklərini müəyyənləşdirməli və sənədləşdirməli və bu öhdəlikləri qarşılayacaq vasitələri təmin etməlidir.
A.7.3.2	FEM subyektləri üçün məlumatların müəyyən edilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərinə öz FEM-nin emalı ilə bağlı veriləcək məlumatları və bu cür təminatın vaxtını müəyyənləşdirməli və sənədləşdirməlidir.
A.7.3.3	FEM subyektlərinə məlumatların təqdim edilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərini FEM nəzarətçisini eyniləşdirən və onların FEM-nin emalını təsvir edən aydın və asanlıqla əlçatan məlumatlarla təmin etməlidir.
A.7.3.4	Razılığın dəyişdirilməsi və ya geri götürülməsi mexanizminin təmin edilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərini razılıqlarını dəyişdirmək və ya geri götürmək üçün mexanizm təmin etməlidir.
A.7.3.5	FEM-in emalına etiraz mexanizminin təmin edilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərini öz FEM-nin emalına etiraz etmək üçün mexanizmlə təmin etməlidir.
A.7.3.6	Məlumatlara çıxış imkanı, onların düzəldilməsi və/və ya silinməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərinin öz FEM-nə daxil olması, düzəliş etməsi və/və ya silməsi öhdəliklərini qarşılamaq üçün siyasətlər, prosedurlar və/və ya mexanizmlər tətbiq etməlidir.
A.7.3.7	FEM nəzarətçilərinin üçüncü tərəfləri məlumatlandırmaq öhdəlikləri	*Nəzarət tədbiri* Təşkilat FEM-in paylaşıldığı üçüncü tərəfləri paylaşılan FEM-lə bağlı hər hansı dəyişiklik, razılığın geri götürülməsi və ya etirazlar barədə məlumatlandırmalı və bunu həyata keçirmək üçün müvafiq siyasətlər, prosedurlar və/və ya mexanizmlər icra etməlidir.
A.7.3.8	Emal edilən FEM-in surətinin təmin edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in subyekti tələb etdikdə emal edilən FEM-in surətini təmin edə bilməlidir.
A.7.3.9	Müraciətlərin emal edilməsi	*Nəzarət tədbiri* Təşkilat FEM subyektlərinin qanuni müraciətlərinin idarə edilməsinə və ona cavab verilməsinə yönəlmiş siyasətləri və prosedurları müəyyənləşdirməli və sənədləşdirməlidir.
A.7.3.10	Avtomatik qərar qəbulu	*Nəzarət tədbiri* Təşkilat yalnız FEM-in avtomatik emalına əsaslanan və təşkilatın FEM-in subyekti ilə bağlı verdiyi qərarlardan qaynaqlanan FEM subyektləri qarşısındakı öhdəlikləri, o cümlədən hüquqi öhdəlikləri müəyyənləşdirməli və nəzərə almalıdır.

Cədvəl A.1 *(davamı)*

A.7.4 Layihəyə görə və standart parametrlərə görə şəxsi həyatın toxunulmazlığı Məqsəd: Proseslərin və sistemlərin məlumatların toplanması və emalının (o cümlədən istifadə, açıqlanma, saxlanılma, ötürülmə və məhv edilmə) müəyyən edilən məqsəd üçün lazım olan səviyyə ilə məhdudlaşmasını təmin edəcək formada hazırlanmasını təmin etmək.		
A.7.4.1	Məlumatların toplanmasının məhdudlaşdırılması	*Nəzarət tədbiri* Təşkilat FEM-in toplanılmasını müəyyən edilən məqsədlər üçün müvafiq, proporsional və zəruri olan minimum səviyyə ilə məhdudlaşdırmalıdır.
A.7.4.2	Məlumatların emalının məhdudlaşdırılması	*Nəzarət tədbiri* Təşkilat FEM-in emalını müəyyən edilən məqsədlər üçün adekvat, müvafiq və zəruri olan səviyyə ilə məhdudlaşdırmalıdır.
A.7.4.3	Dəqiqlik və keyfiyyət	*Nəzarət tədbiri* Təşkilat FEM-in emal edilmə dövrü boyunca FEM-in emal edildiyi məqsədlər üçün lazım olduğu qədər dəqiq, tam və müasir olmasını təmin etməli və sənədləşdirməlidir.
A.7.4.4	FEM-in azaldılması məqsədləri	*Nəzarət tədbiri* Təşkilat məlumatların azaldılması məqsədlərini və həmin məqsədlərə çatmaq üçün hansı mexanizmlərin (məs., adsızlaşdırılma) istifadə olunmasını müəyyənləşdirməli və sənədləşdirməlidir.
A.7.4.5	Emalın sonunda FEM-in adsızlaşdırılması və silinməsi	*Nəzarət tədbiri* Təşkilat ilkin FEM müəyyən edilən məqsəd (məqsədlər) üçün artıq lazım olmayanda, FEM-i silməli və ya FEM subyektlərinin identifikasiyasına və ya yenidən identifikasiyasına imkan verməyəcək formaya çevirməlidir.
A.7.4.6	Müvəqqəti fayllar	*Nəzarət tədbiri* Təşkilat FEM-in emalının nəticəsində yaradılan müvəqqəti faylların müəyyənləşdirilən, sənədləşdirilən müddət çərçivəsində sənədləşdirilmiş prosedurlara uyğun olaraq silinməsini (məs., silinməsini və ya məhv edilməsini) təmin etməlidir.
A.7.4.7	Məlumatların saxlanması	*Nəzarət tədbiri* Təşkilat FEM-i emal edildiyi məqsədlər üçün lazım olan müddətdən daha uzun müddət ərzində saxlamamalıdır.
A.7.4.8	Məlumatların məhv edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in məhv edilməsi üçün sənədləşdirilən siyasətlərə, prosedurlara və/və ya mexanizmlərə sahib olmalıdır.
A.7.4.9	FEM-in ötürülməsinə nəzarət tədbirləri	*Nəzarət tədbiri* Təşkilat məlumatların ötürülməsi şəbəkəsi ilə ötürülən FEM-i (məs., başqa bir təşkilata göndərilən) məlumatların nəzərdə tutulan təyinat nöqtəsinə çatmasını təmin etmək üçün hazırlanan müvafiq nəzarət tədbirlərinə cəlb etməlidir.
A.7.5 FEM-in paylaşılması, ötürülməsi və açıqlanması Məqsəd: FEM-in paylaşılıb-paylaşılmadığını, başqa yurisdiksiyalara və ya üçüncü tərəflərə ötürülüb-ötürülmədiyini və/və ya müvafiq öhdəliklərə uyğun olaraq açıqlanıb-açıqlanmadığını müəyyənləşdirmək və sənədləşdirmək.		
A.7.5.1	FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsasın müəyyən edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in yurisdiksiyalar arasında ötürülməsi üçün müvafiq əsası müəyyənləşdirməli və sənədləşdirməlidir.
A.7.5.2	FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar	*Nəzarət tədbiri* Təşkilat FEM-in ötürülə biləcəyi ölkələri və beynəlxalq təşkilatları dəqiqliklə müəyyənləşdirməli və sənədləşdirməlidir.

Cədvəl A.1 *(davamı)*

A.7.5.3	FEM-in ötürülməsinə dair qeydlər	*Nəzarət tədbiri* Təşkilat FEM-in üçüncü tərəflərə və ya üçüncü tərəflərdən ötürülmə əməliyyatlarını qeyd etməli və FEM subyektləri qarşısında olan öhdəlikləri ilə bağlı gələcək müraciətləri dəstəkləmək üçün bu tərəflərlə əməkdaşlığı təmin etməlidir.
A.7.5.4	FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər	*Nəzarət tədbiri* Təşkilat FEM-in üçüncü tərəflərə açıqlanmasını, o cümlədən hansı FEM-in açıqlandığını, kimə və nə vaxt açıqlandığını qeyd etməlidir.

Qoşma B
(normativ)

FMİS-ə aid nəzarət məqsədləri və nəzarət tədbirləri (FEM-i emal edən tərəflər)

Bu Qoşma FEM subpodratçılarından istifadə edən və ya istifadə etməyən FEM-i emal edən tərəflər kimi çıxış edən təşkilatlar üçün nəzərdə tutulub. O, ISO/IEC 27001:2013 standartındakı Qoşma A-nı daha geniş formatda təqdim edir.

Cədvəl B.1-də sadalanan əlavə və ya dəyişdirilmiş nəzarət məqsədləri və nəzarət tədbirləri birbaşa olaraq bu sənəddə müəyyənləşdirilən nəzarət məqsədlərindən və nəzarət tədbirlərindən irəli gəlir və onlarla uzlaşır və ISO/IEC 27001:2013 standartının 5.4.1.3 bəndində təkmilləşdirilən 6.1.3 bəndi kontekstində istifadə edilməlidir.

Bu Qoşmada sadalanan nəzarət məqsədlərinin və nəzarət tədbirlərinin hamısının FMİS-in icrasına daxil edilməsinə ehtiyac yoxdur. İstisna edilən hər hansı nəzarət məqsədlərinin əsaslandırılması Tətbiq Bəyanatına daxil edilməlidir (baxın:5.4.1.3). İstisna üçün əsaslandırmaya nəzarət tədbirlərinin risklərin qiymətləndirilməsinə görə zəruri hesab edilmədiyi və tətbiq olunan qanunvericilik və/və ya normativ aktların tələb etmədiyi (və ya istisnalara məruz qaldığı) hallar daxil ola bilər.

QEYD: Bu Qoşmadakı maddə nömrələri Maddə 8-dəki bənd nömrələri ilə əlaqəlidir.

Cədvəl B.1 — Nəzarət məqsədləri və nəzarət tədbirləri

B.8.2 Məlumatların toplanması və emalı şərtləri Məqsəd: Emal prosesinin qanuni olduğunu, tətbiq olunan yurisdiksiyalara görə hüquqi əsasının olduğunu və aydın şəkildə müəyyənləşdirilən və qanuni məqsədləri olduğunu müəyyənləşdirmək və sənədləşdirmək.		
B.8.2.1	Müştəri ilə müqavilə	*Nəzarət tədbiri* Təşkilat müvafiq halda FEM-in emalı ilə bağlı müqavilənin müştərinin öhdəliklərinə yardımın təmin edilməsində təşkilatın rolunu nəzərə almasını təmin etməlidir (emalın xarakterini və təşkilat üçün əlçatan olan məlumatları nəzərə alaraq).
B.8.2.2	Təşkilatın məqsədləri	*Nəzarət tədbiri* Təşkilat müştəri adından emal edilən FEM-in yalnız müştərinin sənədləşdirilmiş təlimatlarında göstərilən məqsədlər üçün emal edilməsini təmin etməlidir.
B.8.2.3	Marketinq və reklam məqsədilə istifadə	*Nəzarət tədbiri* Təşkilat FEM-in müvafiq subyektindən əvvəlcədən razılıq alındığını müəyyənləşdirmədən müqavilə çərçivəsində emal edilən FEM-i marketinq və reklam məqsədi ilə istifadə etməməlidir. Təşkilat bu cür razılığı verməyi xidmətin alınması üçün şərtə çevirməməlidir.
B.8.2.4	Pozuntuya yol verən təlimat	*Nəzarət tədbiri* Təşkilat emal təlimatının tətbiq olunan qanunvericiliyi və/və ya normativ aktları pozduğunu düşünürsə, müştərini məlumatlandırmalıdır.
B.8.2.5	Müştərinin öhdəlikləri	*Nəzarət tədbiri* Təşkilat müştərini müvafiq məlumatlarla təmin etməlidir ki, müştəri öz öhdəliklərinə əməl etdiyini göstərə bilsin.

Cədvəl B.1 *(davamı)*

B.8.2.6	FEM-in emalı ilə əlaqəli qeydlər	*Nəzarət tədbiri* Təşkilat müştəri adına həyata keçirilən FEM-in emalı üçün öz öhdəliklərinə (müvafiq müqavilədə müəyyənləşdirildiyi kimi) əməl etməyini nümayiş etdirmək məqsədilə lazımi qeydləri müəyyənləşdirməli və saxlamalıdır.
B.8.3 FEM subyektləri qarşısında öhdəliklər Məqsəd: FEM subyektlərinə özlərinin FEM-nin emalı barədə müvafiq məlumatların verilməsini təmin etmək və FEM subyektləri qarşısında FEM-in emalı ilə bağlı hər hansı digər müvafiq öhdəlikləri yerinə yetirmək.		
B.8.3.1	FEM subyektləri qarşısında öhdəliklər	*Nəzarət tədbiri* Təşkilat müştərini FEM subyektləri ilə bağlı öhdəliklərinə əməl etmək üçün vasitələrlə təmin etməlidir.
B.8.4 Layihəyə görə və standart parametrlərə görə şəxsi həyatın toxunulmazlığı Məqsəd: Proseslərin və sistemlərin FEM-in toplanması və emalının (o cümlədən istifadə, açıqlanma, saxlanılma, ötürülmə və məhv edilmə) müəyyən edilən məqsəd üçün lazım olan səviyyə ilə məhdudlaşmasını təmin edəcək formada hazırlanmasını təmin etmək.		
B.8.4.1	Müvəqqəti fayllar	*Nəzarət tədbiri* Təşkilat FEM-in emalının nəticəsində yaradılan müvəqqəti faylların müəyyənləşdirilən, sənədləşdirilən müddət çərçivəsində sənədləşdirilmiş prosedurlara uyğun olaraq silinməsini (məs., silinməsini və ya məhv edilməsini) təmin etməlidir.
B.8.4.2	FEM-in qaytarılması, ötürülməsi və ya məhv edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in təhlükəsiz şəkildə qaytarıla, ötürülə və/və ya məhv edilə bilməsini təmin etməlidir. Bu, onun siyasətini müştəri üçün də əlçatan etməlidir.
B.8.4.3	FEM-in ötürülməsinə nəzarət tədbirləri	*Nəzarət tədbiri* Təşkilat məlumatların ötürülməsi şəbəkəsi ilə ötürülən FEM-i məlumatların nəzərdə tutulan təyinat nöqtəsinə çatmasını təmin etmək üçün hazırlanan müvafiq nəzarət tədbirlərinə müvafiq şəkildə ötürməlidir.
B.8.5 FEM-in paylaşılması, ötürülməsi və açıqlanması Məqsəd: FEM-in paylaşılıb-paylaşılmadığını, başqa yurisdiksiyalara və ya üçüncü tərəflərə ötürülüb-ötürülmədiyini və/və ya müvafiq öhdəliklərə uyğun olaraq açıqlanıb-açıqlanmadığını müəyyənləşdirmək və sənədləşdirmək.		
B.8.5.1	FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsas	*Nəzarət tədbiri* Təşkilat müştərini FEM-in yurisdiksiyalar arasında ötürülməsi əməliyyatlarının əsası və bu baxımdan edilməsi nəzərdə tutulan hər hansı dəyişikliklər barədə vaxtında məlumatlandırmalıdır ki, müştəri bu cür dəyişikliklərə etiraz edə və ya müqaviləyə xitam verə bilsin.
B.8.5.2	FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar	*Nəzarət tədbiri* Təşkilat FEM-in ötürülə biləcəyi ölkələri və beynəlxalq təşkilatları dəqiqliklə müəyyənləşdirməli və sənədləşdirməlidir.
B.8.5.3	FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər	*Nəzarət tədbiri* Təşkilat FEM-in üçüncü tərəflərə açıqlanması hallarını, o cümlədən hansı FEM-in açıqlandığını, kimə və nə vaxt açıqlandığını qeyd etməlidir.
B.8.5.4	FEM-in açıqlanması ilə bağlı sorğuların bildirilməsi	*Nəzarət tədbiri* Təşkilat FEM-in açıqlanması üçün hüquqi öhdəlik yaradan hər hansı müraciətləri müştəriyə bildirməlidir.

Cədvəl B.1 *(davamı)*

B.8.5.5	FEM-in açıqlanmasının hüquqi öhdəlik yaratdığı hallar	*Nəzarət tədbiri* Təşkilat FEM-in hüquqi öhdəlik yaratmayan açıqlanma hallarına dair hər hansı müraciətlərdən imtina etməli, hər hansı FEM-i açıqlamazdan əvvəl müvafiq müştəri ilə məsləhətləşməli və müvafiq müştərinin icazə verdiyi FEM-in açıqlanması üçün müqavilə ilə razılaşdırılan tələbləri qəbul etməlidir.
B.8.5.6	FEM-in emalı üçün istifadə edilən subpodratçıların açıqlanması	*Nəzarət tədbiri* Təşkilat FEM-in emalı üçün hər hansı subpodratçılardan istifadə etməzdən əvvəl subpodratçıdan istifadə barədə müştəriyə xəbər verməlidir.
B.8.5.7	FEM-in emalı üçün subpodratçının cəlb edilməsi	*Nəzarət tədbiri* Təşkilat FEM-in emalı üçün subpodratçını yalnız müştəri müqaviləsinə əsasən cəlb etməlidir.
B.8.5.8	FEM-in emalı üçün subpodratçının dəyişdirilməsi	*Nəzarət tədbiri* Ümumi yazılı icazə olduğu halda, təşkilat FEM-in emalı üçün subpodratçıların əlavə edilməsi və ya dəyişdirilməsi ilə bağlı nəzərdə tutulan hər hansı dəyişikliklər barədə müştərini məlumatlandırmalı, bununla müştəriyə bu cür dəyişikliklərə etiraz etmək imkanı verməlidir.

Qoşma C
(informativ)

ISO/IEC 29100 standartına uyğun strukturlaşdırma

Cədvəl C.1 və C.2-də bu sənədin müddəaları ilə ISO/IEC 29100 standartının şəxsi həyatın toxunulmazlığı prinsipləri arasında strukturlaşdırılmış uyğunlaşma təqdim olunur. O, bu sənədin tələblərinə və nəzarət tədbirlərinə əməl edilməsinin ISO/IEC 29100 standartındakı ümumi şəxsi həyatın toxunulmazlığı prinsipləri ilə necə əlaqəli olduğunu sırf göstərici formasında təqdim edir.

Cədvəl C.1 — FEM nəzarətçiləri və ISO/IEC 29100 standartı üzrə nəzarət tədbirlərinin strukturlaşdırılması

ISO/IEC 29100 standartının şəxsi həyatın toxunulmazlığı prinsipləri	FEM nəzarətçiləri üçün müvafiq nəzarət tədbirləri
1. Razılıq və Seçim	A.7.2.1 Məqsədin müəyyənləşdirilməsi və sənədləşdirilməsi A.7.2.2 Hüquqi əsasın müəyyən edilməsi A.7.2.3 Razılığın nə vaxt və necə alınacağının müəyyən edilməsi A.7.2.4 Razılığın əldə edilməsi və qeydə alınması A.7.2.5 Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi A.7.3.4 Razılığın dəyişdirilməsi və ya geri götürülməsi mexanizminin təmin edilməsi A.7.3.5 FEM-in emalına etiraz mexanizminin təmin edilməsi A.7.3.7 FEM nəzarətçilərinin üçüncü tərəfləri məlumatlandırmaq öhdəlikləri
2. Məqsədin etibarlılığı və aydınlaşdırılması	A.7.2.1 Məqsədin müəyyənləşdirilməsi və sənədləşdirilməsi A.7.2.2 Hüquqi əsasın müəyyən edilməsi A.7.2.5 Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi A.7.3.2 FEM subyektləri üçün məlumatların müəyyən edilməsi A.7.3.3 FEM subyektlərinə məlumatların təqdim edilməsi A.7.3.10 Avtomatik qərar qəbulu
3. Məlumatların toplanmasının məhdudlaşdırılması	A.7.2.5 Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi A.7.4.1 Məlumatların toplanmasının məhdudlaşdırılması
4. Məlumatların azaldılması	A.7.4.2 Məlumatların emalının məhdudlaşdırılması A.7.4.4 FEM-in azaldılması məqsədləri A.7.4.5 Emalın sonunda FEM-in adsızlaşdırılması və silinməsi
5. Məlumatların istifadəsi, saxlanması və açıqlanmasının məhdudlaşdırılması	A.7.4.4 FEM-in azaldılması məqsədləri A.7.4.5 Emalın sonunda FEM-in adsızlaşdırılması və silinməsi A.7.4.6 Müvəqqəti fayllar A.7.4.7 Məlumatların saxlanması A.7.4.8 Məlumatların məhv edilməsi A.7.5.1 FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsasın müəyyən edilməsi A.7.5.4 FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər
6.Dəqiqlik və keyfiyyət	A.7.4.3 Dəqiqlik və keyfiyyət
7. Açıqlıq, şəffaflıq və bildiriş verilməsi	A.7.3.2 FEM subyektləri üçün məlumatların müəyyən edilməsi A.7.3.3 FEM subyektlərinə məlumatların təqdim edilməsi

Cədvəl C.1 *(davamı)*

ISO/IEC 29100 standartının şəxsi həyatın toxunulmazlığı prinsipləri	FEM nəzarətçiləri üçün müvafiq nəzarət tədbirləri
8. Fərdi iştirak və çıxış imkanı	A.7.3.1 FEM subyektləri qarşısında öhdəliklərin müəyyən edilməsi və yerinə yetirilməsi A.7.3.3 Emal edilən FEM-in surətinin təmin edilməsi A.7.3.6 Məlumatlara çıxış imkanı, onların düzəldilməsi və/və ya silinməsi A.7.3.8 Emal edilən FEM-in surətinin təmin edilməsi A.7.3.9 Müraciətlərin emal edilməsi
9. Hesabatlılıq	A.7.2.6 FEM-i emal edən tərəflərlə müqavilələr A.7.2.7 Birgə nəzarətçi A.7.2.8 FEM-in emalı ilə əlaqəli qeydlər A.7.3.9 Müraciətlərin emal edilməsi A.7.5.1 FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsasın müəyyən edilməsi A.7.5.2 FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar A.7.5.3 FEM-in ötürülməsinə dair qeydlər
10. İnformasiya Təhlükəsizliyi	A.7.2.6 FEM-i emal edən tərəflərlə müqavilələr A.7.4.9 FEM-in ötürülməsinə nəzarət tədbirləri
11. Şəxsi həyatın toxunulmazlığına uyğunluq	A.7.2.5 Şəxsi həyatın toxunulmazlığına təsirin qiymətləndirilməsi

Cədvəl C.2 — FEM-i emal edən tərəflər və ISO/IEC 29100 standartı üzrə nəzarət tədbirlərinin strukturlaşdırılması

ISO/IEC 29100 standartının şəxsi həyatın toxunulmazlığı prinsipləri	FEM-i emal edən tərəflər üçün müvafiq nəzarət tədbirləri
1. Razılıq və Seçim	B.8.2.5 Müştərinin öhdəlikləri
2. Məqsədin etibarlılığı və aydınlaşdırılması	B.8.2.1 Müştəri ilə müqavilə B.8.2.2 Təşkilatın məqsədləri B.8.2.3 Marketinq və reklam məqsədilə istifadə B.8.2.4 Pozuntuya yol verən təlimat B.8.3.1 FEM subyektləri qarşısında öhdəliklər
3. Məlumatların toplanmasının məhdudlaşdırılması	M/D
4. Məlumatların azaldılması	B.8.4.1 Müvəqqəti fayllar
5. İstifadənin, saxlanmanın və məlumatların açıqlanmasının məhdudlaşdırılması	B.8.5.3 FEM-in üçüncü tərəflərə açıqlanması ilə bağlı qeydlər B.8.5.4 FEM-in açıqlanması ilə bağlı sorğuların bildirilməsi B.8.5.5 FEM-in açıqlanmasının hüquqi öhdəlik yaratdığı hallar
6.Dəqiqlik və keyfiyyət	M/D
7. Açıqlıq, şəffaflıq və bildiriş verilməsi	B.8.5.6 FEM-in emalı üçün istifadə edilən subpodratçıların açıqlanması B.8.5.7 FEM-in emalı üçün subpodratçının cəlb edilməsi B.8.5.8 FEM-in emalı üçün subpodratçının dəyişdirilməsi
8. Fərdi iştirak və çıxış imkanı	B.8.3.1 FEM subyektləri qarşısında öhdəliklər
9. Hesabatlılıq	B.8.2.6 FEM-in emalı ilə əlaqəli qeydlər B.8.4.2 FEM-in qaytarılması, ötürülməsi və ya məhv edilməsi B.8.5.1 FEM-in yurisdiksiyalar arasında ötürülməsi üçün əsasın müəyyən edilməsi B.8.5.2 FEM-in ötürülə biləcəyi ölkələr və beynəlxalq təşkilatlar
10. İnformasiya Təhlükəsizliyi	B.8.4.3 FEM-in ötürülməsinə nəzarət tədbirləri
11. Şəxsi həyatın toxunulmazlığına uyğunluq	B.8.2.5 Müştərinin öhdəlikləri

Qoşma D
(informativ)

Aİ-nin Fərdi Məlumatların Mühafizəsinə dair Ümumi Qaydalarına uyğun strukturlaşdırma

Bu Qoşma bu sənədin müddəaları ilə Aİ-nin Fərdi Məlumatların Mühafizəsinə dair Ümumi Qaydalarının 5-49-cu Maddələri (43.Maddə istisna olmaqla) arasında göstərici xarakterli strukturlaşdırmanı təmin edir. O, bu sənədin tələblərinə və nəzarət tədbirlərinə əməl edilməsinin Aİ-nin Fərdi Məlumatların Mühafizəsinə dair Ümumi Qaydaları (GDPR) ilə nəzərdə tutulmuş öhdəlikləri yerinə yetirmək üçün necə münasib ola biləcəyini göstərir.

Lakin bu, sırf göstərici xarakterlidir və bu sənədə görə, hüquqi məsuliyyətlərini qiymətləndirmək və onlara necə əməl ediləcəyinə qərar vermək təşkilatların məsuliyyətinə daxildir.

Cədvəl D.1 — ISO/IEC 27701 strukturunun GDPR maddələrinə uyğun strukturlaşdırılması

Bu sənədin bəndi	GDPR maddələri
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)
6.8.2.7	(5)(1)(f)
6.8.2.9	(5)(1)(f)
6.9.3.1	(5)(1)(f), (32)(1)(c)
6.9.4.1	(5)(1)(f)
6.9.4.2	(5)(1)(f)
6.10.2.1	(5)(1)(f)

Cədvəl D.1 *(davamı)*

Bu sənədin bəndi	GDPR maddələri
6.10.2.4	(5)(1)(f), (28)(3)(b), (38)(5)
6.11.1.2	(5)(1)(f), (32)(1)(a)
6.11.2.1	(25)(1)
6.11.2.5	(25)(1)
6.11.3.1	(5)(1)(f)
6.12.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.13.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
6.13.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
6.15.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
6.15.1.3	(5)(2), (24)(2)
6.15.2.1	(32)(1)(d), (32)(2)
6.15.2.3	(32)(1)(d), (32)(2)
7.2.1	(5)(1)(b), (32)(4)
7.2.2	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
7.2.3	(8)(1), (8)(2)
7.2.4	(7)(1), (7)(2), (9)(2)(a)
7.2.5	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
7.2.6	(5)(2), (28)(3)(e), (28)(9)
7.2.7	(26)(1), (26)(2), (26)(3)
7.2.8	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
7.3.1	(12)(2)
7.3.2	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)
7.3.3	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
7.3.4	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
7.3.5	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
7.3.6	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
7.3.7	(19)
7.3.8	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
7.3.9	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
7.3.10	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
7.4.1	(5)(1)(b), (5)(1)(c)

Cədvəl D.1 *(davamı)*

Bu sənədin bəndi	GDPR maddələri
7.4.2	(25)(2)
7.4.3	(5)(1)(d)
7.4.4	(5)(1)(c), (5)(1)(e)
7.4.5	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
7.4.6	(5)(1)(c)
7.4.7	(13)(2)(a), (14)(2)(a)
7.4.8	(5)(1)(f)
7.4.9	(5)(1)(f)
7.5.1	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
7.5.2	(15)(2), (30)(1)(e)
7.5.3	(30)(1)(e)
7.5.4	(30)(1)(d)
8.2.1	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
8.2.2	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
8.2.3	(7)(4)
8.2.4	(28)(3)(h)
8.2.5	(28)(3)(h)
8.2.6	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
8.3.1	(15)(3), (17)(2), (28)(3)(e)
8.4.1	(5)(1)(c)
8.4.2	(28)(3)(g), (30)(1)(f)
8.4.3	(5)(1)(f)
8.5.1	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
8.5.2	(30)(2)(c)
8.5.3	(30)(1)(d)
8.5.4	(28)(3)(a)
8.5.5	(48)
8.5.6	(28)(2), (28)(4)
8.5.7	(28)(2), (28)(3)(d)
8.5.8	(28)(2)

Qoşma E
(informativ)

ISO/IEC 27018 və ISO/IEC 29151 standartlarına uyğun strukturlaşdırma

ISO/IEC 27018 FEM-i emal edən tərəflər kimi çıxış edən və ictimai bulud xidmətləri təmin edən təşkilatlar üçün əlavə məlumatlar təqdim edir. ISO/IEC 29151 FEM nəzarətçilərinin FEM-i emal etməsi üçün əlavə nəzarət tədbirləri və göstərişlər təqdim edir.

Cədvəl C.1-də bu sənədin müddəaları ilə ISO/IEC 27018 və ISO/IEC 29151 standartlarının müddəaları arasında göstərici xarakterli strukturlaşdırma təqdim olunur. O, bu sənədin tələblərinin və nəzarət tədbirlərinin ISO/IEC 27018 və/və ya ISO/IEC 29151 standartlarının müddəaları ilə necə uyğunlaşdırıla biləcəyini göstərir.

Bu qoşma sırf göstərici xarakterlidir və müddəalar arasında verilən əlaqə ekvivalentlik kimi nəzərdən keçirilməməlidir.

Cədvəl E.1 — ISO/IEC 27701 standartının ISO/IEC 27018 və ISO/IEC 29151 standartlarına uyğun strukturlaşdırılması

Bu sənədin bəndi	ISO/IEC 27018 standartının bəndi	ISO/IEC 29151 standartının bəndi
5.2	M/D	M/D
5.3	M/D	M/D
5.4	M/D	4.2
5.5	M/D	7.2.3
5.6	M/D	M/D
5.7	M/D	M/D
5.8	M/D	M/D
6.1	M/D	M/D
6.2	5.1.1	5
6.3	6.1.1	M/D
6.4	7.2.2	M/D
6.5.1	M/D	8.1
6.5.2	M/D	8.2
6.5.3	A.11.4, A.11.5	8.3
6.6.1	M/D	M/D
6.6.2	9.2.1, A.11.8, A,11,9, A.11.10	9.2
6.6.3	M/D	9.3
6.6.4	7.2.2, 9.4.2	9.4
6.7	10.1.1	M/D
6.8.1	M/D	11.1
6.8.2	11.2.7, A.11.2, A.11.13	M/D
6.9.1	M/D	12.1
6.9.2	M/D	12,2
6.9.3	M/D	12.3
6.9.4	12.4.1, 12.4.2	12.4
6.9.5	M/D	M/D
6.9.6	M/D	M/D

Cədvəl E.1 *(davamı)*

Bu sənədin bəndi	ISO/IEC 27018 standartının bəndi	ISO/IEC 29151 standartının bəndi
6.9.7	M/D	M/D
6.10.1	M/D	13.1
6.10.2	13.2.1, A.11.1	13.2
6.11.1	A.11.6	M/D
6.11.2	M/D	M/D
6.11.3	12.1.4	M/D
6.12.1	A.11.11	M/D
6.12.2	M/D	M/D
6.13	16.1.1, A.10.1	M/D
6.14	M/D	M/D
6.15.1	A.10.2	M/D
6.15.2	18.2.1	18.2
7.2.1	M/D	A.4
7.2.2	M/D	A.4.1
7.2.3	M/D	M/D
7.2.4	M/D	A.3.1
7.2.5	M/D	A.11.2
7.2.6	M/D	A.11.3
7.2.7	M/D	M/D
7.2.8	M/D	M/D
7.3.1	M/D	A.10
7.3.2	M/D	M/D
7.3.3	M/D	A.9
7.3.4	M/D	M/D
7.3.5	M/D	M/D
7.3.6	M/D	A.10.1
7.3.7	M/D	M/D
7.3.8	M/D	M/D
7.3.9	M/D	M/D
7.3.10	M/D	M/D
7.4.1	M/D	A.5
7.4.2	M/D	M/D
7.4.3	M/D	A.8
7.4.4	M/D	M/D
7.4.5	M/D	A.7.1
7.4.6	M/D	A.7.2
7.4.7	M/D	A.7.1
7.4.8	M/D	M/D
7.4.9	M/D	M/D
7.5.1	M/D	A.13.2
7.5.2	M/D	A.13.2
7.5.3	M/D	A.13.2
7.5.4	M/D	A.7.4

Cədvəl E.1 *(davamı)*

Bu sənədin bəndi	ISO/IEC 27018 standartının bəndi	ISO/IEC 29151 standartının bəndi
8.2.1	M/D	M/D
8.2.2	A.3.1	M/D
8.2.3	A.3.2	M/D
8.2.4	M/D	M/D
8.2.5	M/D	M/D
8.2.6	M/D	M/D
8.3.1	A.2.1	M/D
8.4.1	A.5.1	M/D
8.4.2	A.10.3	M/D
8.4.3	A.12.2	M/D
8.5.1	M/D	M/D
8.5.2	A.12.1	M/D
8.5.3	A.6.2	M/D
8.5.4	A.6.1	M/D
8.5.5	A.6.1	M/D
8.5.6	A.8.1	A.7.5
8.5.7	A.8.1	M/D
8.5.8	A.8.1	M/D

Qoşma F
(informativ)

ISO/IEC 27701 standartının ISO/IEC 27001 və ISO/IEC 27002 standartlarına tətbiq edilməsi yolları

F.1 Bu sənədi necə tətbiq etməli

Bu sənəd ISO/IEC 27001:2013 və ISO/IEC 27002:2013 standartlarına əsaslanır və onların tələblərini və göstərişlərini informasiya təhlükəsizliyi ilə yanaşı, potensial olaraq FEM-in emalının təsirinə məruz qalan FEM subyektlərinin şəxsi həyatının toxunulmazlığının qorunmasını nəzərə almaqla genişləndirir. Bu, ISO/IEC 27001 və ya ISO/IEC 27002 standartlarında "informasiya təhlükəsizliyi" terminin istifadə olunduğu yerlərdə onun əvəzinə "informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı" anlayışının tətbiq edilməsi deməkdir.

Cədvəl F.1 bu sənədə tətbiq etmək məqsədilə informasiya təhlükəsizliyi termininin genişləndirilmiş strukturlaşdırılmasını təqdim edir.

Cədvəl F.1 — İnformasiya təhlükəsizliyi termininin şəxsi həyatın toxunulmazlığı termininin əlavə edilməsi ilə strukturlaşdırılması

ISO/IEC 27001	Bu sənəd (əlavə)
informasiya təhlükəsizliyi	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı
informasiya təhlükəsizliyi siyasəti	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı siyasəti
informasiya təhlükəsizliyinin idarə edilməsi	informasiya təhlükəsizliyi və fərdi məlumatların idarə edilməsi
informasiya təhlükəsizliyinin idarə edilməsi sistemi (İTİS)	fərdi məlumatların idarə edilməsi sistemi (FMİS)
informasiya təhlükəsizliyi məqsədləri	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı məqsədləri
informasiya təhlükəsizliyinin effektivliyi	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığının effektivliyi
informasiya təhlükəsizliyi tələbləri	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı tələbləri
informasiya təhlükəsizliyi riskləri	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı riskləri
informasiya təhlükəsizliyi üzrə risklərin qiymətləndirilməsi	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risklərin qiymətləndirilməsi
informasiya təhlükəsizliyi üzrə risklərin aradan qaldırılması	informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risklərin aradan qaldırılması

Mahiyyət etibarilə, bu sənəd FEM emal edilərkən FEM subyektlərinin şəxsi həyatının toxunulmazlığının qorunmasına üç halda tətbiq olunur:

1) Təhlükəsizlik standartlarının olduğu kimi tətbiqi: İstinad edilən standartlar yuxarıda sadalanan terminlərin əlavə edilməsi ilə olduğu kimi tətbiq edilir. Buna görə də, istinad edilən standart təkrarlanmır, yalnız müvafiq maddələrdə qeyd edilir.

2) Təhlükəsizlik standartlarına əlavələr: İstinad edilən standartlar şəxsi həyatın toxunulmazlığına aid əlavə tələblər və ya icra göstərişləri ilə tətbiq edilir.

3) Təhlükəsizlik standartlarının təkmilləşdirilməsi: İstinad edilən standartlar şəxsi həyatın toxunulmazlığına aid tələblər və ya icra göstərişləri ilə təkmilləşdirilir.

F.2 Təhlükəsizlik standartlarının təkmilləşdirilməsinə nümunə

Bu maddə 5.4.1.2 bəndinin ISO/IEC 27001:2013 standartının 6.1.2 bəndinə necə tətbiq olunduğunu təsvir edir.

FEM-in emalı zamanı FEM subyektlərinin şəxsi həyatının toxunulmazlığının qorunması nəzərə alındığı halda ISO/IEC 27001:2013 standartının 6.1.2 bəndi aşağıda altından xətt çəkilmiş mətn formasında dəyişdiriləcək:

6.1.2 İnformasiya təhlükəsizliyi üzrə risklərin qiymətləndirilməsi

Təşkilat aşağıdakıları təmin edən informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risklərin qiymətləndirilməsi prosesini müəyyənləşdirməli və tətbiq etməlidir:

a) aşağıdakıları ehtiva edən informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risk meyarlarını müəyyən etmək və saxlamaq:

   1) riskin qəbul edilməsi meyarları; və

   2) informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risklərin qiymətləndirilməsini həyata keçirmək üçün meyarlar;

b) təkrarlanan informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risk qiymətləndirmələrinin ardıcıl, etibarlı və müqayisə edilə bilən nəticələr verməsini təmin etmək;

c) informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə riskləri müəyyən etmək:

   1) informasiya təhlükəsizliyi və fərdi məlumatların idarə edilməsi sisteminin tətbiq sahəsində məlumatların məxfiliyi, toxunulmazlığı və əlçatanlığının itməsi ilə əlaqəli riskləri müəyyənləşdirmək üçün informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə risklərin qiymətləndirilməsi prosesini tətbiq etmək; və

   2) risk sahiblərini müəyyənləşdirmək;

d) informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə riskləri təhlil etmək:

   1) 6.1.2 c) bəndində müəyyən edilən risklər reallaşacağı halda ortaya çıxa biləcək potensial nəticələri qiymətləndirmək;

   2) 6.1.2 c) 1) bəndində müəyyən edilən risklərin real baş vermə ehtimalını qiymətləndirmək; və

   3) riskin səviyyələrini müəyyənləşdirmək;

e) informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə riskləri qiymətləndirmək:

   1) riskin təhlili nəticələrini 6.1.2 a) bəndində müəyyən edilən risk meyarları ilə müqayisə etmək; və

   2) riskin aradan qaldırılması üçün təhlil edilən riskləri prioritetləşdirmək.

Təşkilat informasiya təhlükəsizliyi və şəxsi həyatın toxunulmazlığı üzrə riskin qiymətləndirilməsi prosesi haqqında sənədləşdirilmiş informasiyanı saxlamalıdır.

Biblioqrafiya

[1] ISO/IEC 19944, *Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use*

[2] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[3] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[4] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[5] ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

[6] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[7] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[8] ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[9] ISO/IEC/DIS 29184, *Information technology — Security techniques — Guidelines for online privacy notices and consent*