Rada
Európskej únie

V Bruseli 18. júla 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	14. júla 2022
Komu:	Generálny sekretariát Rady
Č. dok. Kom.:	C(2022) 4882 final - ANNEX
Predmet:	PRÍLOHA k DELEGOVANÉMU NARIADENIU KOMISIE, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139, pokiaľ ide o požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014, a ktorým sa menia nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014

Delegáciám v prílohe zasielame dokument C(2022) 4882 final - ANNEX.

Príloha: C(2022) 4882 final - ANNEX

EURÓPSKA
KOMISIA

V Bruseli 14. 7. 2022
C(2022) 4882 final

ANNEX

PRÍLOHA

k

DELEGOVANÉMU NARIADENIU KOMISIE,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139, pokiaľ ide o požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014, a ktorým sa menia nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014

PRÍLOHA

INFORMAČNÁ BEZPEČNOSŤ – ORGANIZAČNÉ POŽIADAVKY

[ČASŤ IS.D.OR]

IS.D.OR.100. Rozsah pôsobnosti

V tejto časti sa stanovujú požiadavky, ktoré musia spĺňať organizácie uvedené v článku 2 tohto nariadenia.

IS.D.OR.200. Systém riadenia informačnej bezpečnosti (ISMS)

a) Na dosiahnutie cieľov stanovených v článku 1 organizácia zriadi, vykonáva a udržiava systém riadenia informačnej bezpečnosti (ISMS), ktorý zabezpečí, aby organizácia:

   1. stanovila politiku v oblasti informačnej bezpečnosti, v ktorej určí celkové zásady organizácie, pokiaľ ide o potenciálny vplyv rizík v oblasti informačnej bezpečnosti na bezpečnosť letectva;

   2. identifikovala a preskúmala riziká v oblasti informačnej bezpečnosti v súlade s ustanovením IS.D.OR.205;

3. určila a vykonávala opatrenia na riešenie rizík v oblasti informačnej bezpečnosti v súlade s ustanovením IS.D.OR.210;

4. zaviedla systém interného nahlasovania informačnej bezpečnosti v súlade s ustanovením IS.D.OR.215;

5. vymedzila a vykonávala v súlade s ustanovením IS.D.OR.220 opatrenia potrebné na odhaľovanie udalostí v oblasti informačnej bezpečnosti, identifikovala tie udalosti, ktoré sa považujú za incidenty s potenciálnym vplyvom na bezpečnosť letectva, s výnimkou prípadov povolených v ustanovení IS.D.OR.205 písm. e), a reagovala na uvedené incidenty v oblasti informačnej bezpečnosti a aby sa z uvedených incidentov zotavila;

6. vykonávala opatrenia, ktoré oznámil príslušný orgán ako okamžitú reakciu na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva;

7. prijímala vhodné opatrenia v súlade s ustanovením IS.D.OR.225 s cieľom riešiť zistenia oznámené príslušným orgánom;

8. vykonávala systém externého nahlasovania v súlade s ustanovením IS.D.OR.230 s cieľom umožniť príslušnému orgánu prijať vhodné opatrenia;

9. spĺňala požiadavky uvedené v ustanovení IS.D.OR.235 pri zadávaní akejkoľvek časti činností uvedených v ustanovení IS.D.OR.200 iným organizáciám;

10. spĺňala požiadavky na personál určené v ustanovení IS.D.OR.240;

11. spĺňala požiadavky na vedenie záznamov určené v ustanovení IS.D.OR.245;

12. monitorovala dodržiavanie požiadaviek tohto nariadenia zo strany organizácie a poskytovala spätnú väzbu o zisteniach zodpovednému manažérovi alebo v prípade projekčných organizácií vedúcemu projekčnej organizácie s cieľom zabezpečiť účinné vykonávanie nápravných opatrení;

13. bez toho, aby boli dotknuté príslušné požiadavky na nahlasovanie incidentov, chránila dôvernosť všetkých informácií, ktoré organizácia mohla získať od iných organizácií, podľa úrovne ich citlivosti.

b) V záujme nepretržitého plnenia požiadaviek uvedených v článku 1 musí organizácia zaviesť postup neustáleho zlepšovania v súlade s ustanovením IS.D.OR.260.

c) Organizácia musí v súlade s ustanovením IS.D.OR.250 dokumentovať všetky kľúčové procesy, postupy, úlohy a zodpovednosti požadované na dosiahnutie súladu s ustanovením IS.D.OR.200 písm. a) a zaviesť postup zmeny tejto dokumentácie. Zmeny týchto procesov, postupov, úloh a zodpovedností sa riadia v súlade s ustanovením IS.D.OR.255.

d) Procesy, postupy, úlohy a zodpovednosti stanovené organizáciou s cieľom dosiahnuť súlad s ustanovením IS.D.OR.200 písm. a) musia zodpovedať povahe a zložitosti jej

činností na základe posúdenia rizík v oblasti informačnej bezpečnosti, ktoré sú vlastné týmto činnostiam, a môžu byť začlenené do iných existujúcich systémov riadenia, ktoré už organizácia zaviedla.

e) Bez toho, aby bola dotknutá povinnosť dodržiavať požiadavky na podávanie správ uvedené v nariadení (EÚ) č. 376/2014[1] a požiadavky uvedené v ustanovení IS.D.OR.200 písm. a) bode 13, môže príslušný orgán udeliť organizácii súhlas s nevykonávaním požiadaviek uvedených v písmenách a) až d) a príslušných požiadaviek uvedených v ustanoveniach IS.D.OR.205 až IS.D.OR.260, ak preukáže k spokojnosti uvedeného orgánu, že jej činnosti, zariadenia a zdroje, ako aj služby, ktoré prevádzkuje, poskytuje, prijíma a udržiava, nepredstavujú žiadne riziká v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva, a to ani pre seba, ani pre iné organizácie. Tento súhlas musí vychádzať zo zdokumentovaného posúdenia rizika v oblasti informačnej bezpečnosti, ktoré organizácia alebo tretia strana vykoná v súlade s ustanovením IS.D.OR.205 a ktoré preskúma a schváli jej príslušný orgán.

Zachovanie platnosti tohto súhlasu preskúma príslušný orgán na základe príslušného cyklu auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.

IS.D.OR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

a) Organizácia identifikuje všetky svoje prvky, ktoré by mohli byť vystavené rizikám v oblasti informačnej bezpečnosti. To zahŕňa:

1. činnosti, zariadenia a zdroje organizácie, ako aj služby, ktoré organizácia prevádzkuje, poskytuje, prijíma alebo udržiava;

2. vybavenie, systémy, údaje a informácie, ktoré prispievajú k fungovaniu prvkov uvedených v bode 1.

b) Organizácia identifikuje rozhrania, ktoré má s inými organizáciami a ktoré by mohli viesť k vzájomnému vystaveniu rizikám v oblasti informačnej bezpečnosti.

c) Pokiaľ ide o prvky a rozhrania uvedené v písmenách a) a b), organizácia identifikuje riziká v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva. Za každé identifikované riziko organizácia:

1. priradí úroveň rizika podľa vopred určenej klasifikácie stanovenej organizáciou;

2. spojí každé riziko a jeho úroveň so zodpovedajúcim prvkom alebo rozhraním určeným v súlade s písmenami a) a b).

Vo vopred určenej klasifikácii uvedenej v bode 1 sa zohľadňuje možnosť výskytu

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 376/2014 z 3. apríla 2014 o ohlasovaní udalostí, ich analýze a na ne nadväzujúcich opatreniach v civilnom letectve, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 996/2010 a ktorým sa zrušuje smernica Európskeho parlamentu a Rady 2003/42/ES a nariadenia Komisie (ES) č. 1321/2007 a (ES) č. 1330/2007 (Ú. v. EÚ L 122, 24.4.2014, s. 18).

scenára ohrozenia a závažnosť jeho bezpečnostných dôsledkov. Na základe tejto klasifikácie a s prihliadnutím na to, či organizácia disponuje štruktúrovaným a opakovateľným procesom riadenia rizík pre prevádzku, musí byť organizácia schopná stanoviť, či je riziko prijateľné alebo či je potrebné s ním zaobchádzať v súlade s ustanovením IS.D.OR.210.

S cieľom uľahčiť vzájomnú porovnateľnosť posúdení rizík sa pri priraďovaní úrovne rizika podľa bodu 1 zohľadňujú príslušné informácie získané v koordinácii s organizáciami uvedenými v písmene b).

d) Organizácia preskúma a aktualizuje posúdenie rizika vykonané v súlade s písmenami a), b) a c) v ktorejkoľvek z týchto situácií:

1. došlo k zmene prvkov, ktoré sú vystavené rizikám v oblasti informačnej bezpečnosti;

2. došlo k zmene v rozhraniach medzi organizáciou a inými organizáciami alebo v rizikách oznámených inými organizáciami;

3. došlo k zmene informácií alebo poznatkov použitých na identifikáciu, analýzu a klasifikáciu rizík;

4. analýza incidentov v oblasti informačnej bezpečnosti priniesla poznatky.

IS.D.OR.210. Riešenie rizika v oblasti informačnej bezpečnosti

a) Organizácia vypracuje opatrenia na riešenie neprijateľných rizík identifikovaných v súlade s ustanovením IS.D.OR.205, včas ich vykoná a skontroluje, či si zachovávajú účinnosť. Tieto opatrenia umožnia organizácii:

1. kontrolovať okolnosti, ktoré prispievajú k skutočnému výskytu scenára ohrozenia;

2. znížiť dôsledky na bezpečnosť letectva spojené s realizáciou scenára ohrozenia;

3. vyhýbať sa rizikám.

Týmito opatreniami sa nesmú zavádzať žiadne nové možné neprijateľné riziká pre bezpečnosť letectva.

b) Osoba uvedená v ustanovení IS.D.OR.240 písm. a) a b) a iný dotknutý personál organizácie musia byť informovaní o výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.D.OR.205, zodpovedajúcich scenároch ohrozenia a opatreniach, ktoré sa majú vykonať.

Organizácia musí informovať aj organizácie, s ktorými má rozhranie v súlade s ustanovením IS.D.OR.205 písm. b), o akomkoľvek spoločnom riziku pre obe organizácie.

IS.D.OR.215. Systém interného nahlasovania informačnej bezpečnosti

a) Organizácia zriadi systém interného nahlasovania s cieľom umožniť zhromažďovanie a hodnotenie udalostí v oblasti informačnej bezpečnosti vrátane udalostí, ktoré sa majú nahlasovať podľa ustanovenia IS.D.OR.230.

b) Systém a proces uvedený v ustanovení IS.D.OR.220 musia umožniť organizácii:

1. identifikovať, ktoré z udalostí nahlásených podľa písmena a) sa považujú za incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva;

2. identifikovať príčiny a faktory prispievajúce k incidentom a zraniteľnostiam v oblasti informačnej bezpečnosti identifikovaným v súlade s bodom 1 a riešiť ich ako súčasť procesu riadenia rizík v oblasti informačnej bezpečnosti v súlade s ustanoveniami IS.D.OR.205 a IS.D.OR.220;

3. zabezpečiť hodnotenie všetkých známych relevantných informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti identifikovaných v súlade s bodom 1;

4. zabezpečiť zavedenie metódy interného šírenia informácií podľa potreby.

c) Každá zazmluvnená organizácia, ktorá môže vystaviť organizáciu rizikám v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, je povinná nahlásiť organizácii udalosti v oblasti informačnej bezpečnosti. Uvedené správy sa predkladajú s použitím postupov stanovených v osobitných zmluvných dojednaniach a vyhodnocujú sa v súlade s písmenom b).

d) Organizácia spolupracuje pri vyšetrovaniach s akoukoľvek inou organizáciou, ktorá významne prispieva k informačnej bezpečnosti svojich vlastných činností.

e) Organizácia môže zlúčiť tento systém nahlasovania s inými systémami nahlasovania, ktoré už zaviedla.

IS.D.OR.220. Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a obnova

a) Na základe výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.D.OR.205 a výsledku riešenia rizík vykonaného v súlade s ustanovením IS.D.OR.210 musí organizácia zaviesť opatrenia na odhaľovanie incidentov a zraniteľností, ktoré naznačujú možnú realizáciu neprijateľných rizík a ktoré môžu mať vplyv na bezpečnosť letectva. Uvedené opatrenia na odhaľovanie umožnia organizácii:

1. identifikovať odchýlky od vopred stanovenej základnej funkčnej výkonnosti;

2. spúšťať upozornenia na aktiváciu vhodných reakčných opatrení v prípade akejkoľvek odchýlky.

b) Organizácia musí zaviesť opatrenia s cieľom reagovať na všetky podmienky udalosti

identifikované v súlade s písmenom a), ktoré sa môžu vyvinúť alebo sa vyvinuli do incidentu v oblasti informačnej bezpečnosti. Uvedené opatrenia reakcie umožnia organizácii:

1. iniciovať reakciu na varovania uvedené v písmene a) bode 2 aktivovaním vopred stanovených zdrojov a priebehu činností;

2. obmedziť šírenie útoku a zabrániť úplnej realizácii scenára ohrozenia;

3. regulovať poruchový režim dotknutých prvkov vymedzených v ustanovení IS.D.OR.205 písm. a).

c) Organizácia musí zaviesť opatrenia zamerané na obnovu po incidentoch v oblasti informačnej bezpečnosti vrátane núdzových opatrení, ak je to potrebné. Uvedené opatrenia na obnovu umožnia organizácii:

1. odstrániť stav spôsobený incidentom, alebo ho obmedziť na prípustnú úroveň;

2. dosiahnuť bezpečný stav dotknutých prvkov vymedzených v ustanovení IS.D.OR.205 písm. a) v rámci času na zotavenie, ktorý predtým vymedzila organizácia.

IS.D.OR.225. Reakcia na zistenia oznámené príslušným orgánom

a) Po prijatí oznámenia o zisteniach, ktoré predložil príslušný orgán, musí organizácia:

1. určiť hlavnú príčinu alebo príčiny nesúladu a faktory prispievajúce k nesúladu;

2. stanoviť plán nápravných opatrení;

3. preukázať nápravu nesúladu k spokojnosti príslušného orgánu.

b) Opatrenia uvedené v písmene a) sa vykonajú v lehote dohodnutej s príslušným orgánom.

IS.D.OR.230. Systém externého nahlasovania informačnej bezpečnosti

a) Organizácia musí zaviesť systém nahlasovania informačnej bezpečnosti, ktorý je v súlade s požiadavkami stanovenými v nariadení (EÚ) č. 376/2014 a jeho delegovaných a vykonávacích aktoch, ak sa uvedené nariadenie vzťahuje na organizáciu.

b) Bez toho, aby boli dotknuté povinnosti stanovené v nariadení (EÚ) č. 376/2014, organizácia zabezpečí, aby sa akýkoľvek incident alebo zraniteľnosť v oblasti informačnej bezpečnosti, ktoré môžu predstavovať závažné riziko pre bezpečnosť letectva, nahlásil jej príslušnému orgánu. Okrem toho:

1. ak takýto incident alebo zraniteľnosť ovplyvňuje lietadlo alebo súvisiaci systém či komponent, organizácia to musí nahlásiť aj držiteľovi schválenia projektu;

2. ak takýto incident alebo zraniteľnosť ovplyvňuje systém alebo komponent používaný organizáciou, organizácia to nahlási organizácii zodpovednej za projekt systému alebo komponentu.

c) Organizácia nahlasuje podmienky uvedené v písmene b) takto:

1. oznámenie sa predloží príslušnému orgánu a v prípade potreby držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu hneď, ako sa organizácia dozvie o týchto podmienkach;

2. správa sa predloží príslušnému orgánu a prípadne držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu, a to čo najskôr, najneskôr však do 72 hodín od momentu, keď sa organizácia dozvedela o podmienkach, pokiaľ tomu nebránia výnimočné okolnosti.

Správa sa vypracuje v podobe určenej príslušným orgánom a obsahuje všetky relevantné informácie o podmienkach, ktoré sú organizácii známe;

3. príslušnému orgánu a prípadne držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu sa predloží kontrolná správa, v ktorej sa uvedú podrobnosti o opatreniach, ktoré organizácia prijala alebo plánuje prijať na zotavenie sa z incidentu, a opatrenia, ktoré má v úmysle prijať na zabránenie podobným incidentom v oblasti informačnej bezpečnosti v budúcnosti.

Kontrolná správa sa predloží ihneď po určení týchto opatrení a vypracuje sa v podobe, ktorú určí príslušný orgán.

IS.D.OR.235. Zadávanie činností riadenia informačnej bezpečnosti

a) Organizácia zabezpečí, aby pri zazmluvňovaní akejkoľvek časti činností uvedených v ustanovení IS.D.OR.200 s inými organizáciami boli zazmluvnené činnosti v súlade s požiadavkami tohto nariadenia a aby zazmluvnená organizácia pracovala pod jej dohľadom. Organizácia zabezpečí, aby riziká spojené so zazmluvnenými činnosťami boli primerane riadené.

b) Organizácia zabezpečí príslušnému orgánu na jeho žiadosť prístup k zazmluvnenej organizácii s cieľom určiť, či naďalej spĺňa príslušné požiadavky stanovené v tomto nariadení.

IS.D.OR.240. Požiadavky na personál

a) Zodpovedný manažér organizácie alebo v prípade projekčných organizácií vedúci projekčnej organizácie určený v súlade s nariadením (EÚ) č. 748/2012 a nariadením (EÚ) č. 139/2014, ako sa uvádza v článku 2 ods. 1 písm. a) a b) tohto nariadenia, má podnikovú právomoc na zabezpečenie toho, aby sa všetky činnosti požadované v tomto nariadení mohli financovať a vykonávať. Táto osoba:

1. zabezpečuje, aby boli k dispozícii všetky potrebné zdroje na splnenie požiadaviek tohto nariadenia;

2. stanovuje a presadzuje politiku informačnej bezpečnosti uvedenú v ustanovení IS.D.OR.200 písm. a) bode 1;

3. preukáže základné znalosti o tomto nariadení.

b) Zodpovedný manažér alebo v prípade projekčných organizácií vedúci projekčnej organizácie vymenuje osobu alebo skupinu osôb, aby sa zabezpečilo, že organizácia spĺňa požiadavky tohto nariadenia, a vymedzí rozsah ich právomocí. Uvedená osoba alebo skupina osôb podlieha priamo zodpovednému manažérovi alebo v prípade projekčných organizácií vedúcemu projekčnej organizácie a musí mať primerané znalosti, prax a skúsenosti na plnenie svojich povinností. V postupoch sa určí, kto zastupuje určitú osobu v prípade dlhodobej neprítomnosti uvedenej osoby.

c) Zodpovedný manažér alebo v prípade projekčných organizácií vedúci projekčnej organizácie vymenuje osobu alebo skupinu osôb, ktoré budú zodpovedné za riadenie funkcie monitorovania súladu podľa ustanovenia IS.D.OR.200 písm. a) bodu 12).

d) Ak organizácia zdieľa organizačné štruktúry, politiky, procesy a postupy v oblasti informačnej bezpečnosti s inými organizáciami alebo oblasťami svojej vlastnej organizácie, ktoré nie sú súčasťou schválenia alebo vyhlásenia, zodpovedný manažér alebo v prípade projekčných organizácií vedúci projekčnej organizácie môže delegovať svoje činnosti na spoločnú zodpovednú osobu.

V takom prípade sa stanovia koordinačné opatrenia medzi zodpovedným manažérom organizácie alebo v prípade projekčných organizácií vedúcim projekčnej organizácie a spoločnou zodpovednou osobou s cieľom zabezpečiť primeranú integráciu riadenia informačnej bezpečnosti v rámci organizácie.

e) Zodpovedný manažér alebo vedúci projekčnej organizácie alebo spoločná zodpovedná osoba uvedená v písmene d) majú podnikovú právomoc zriadiť a udržiavať organizačné štruktúry, politiky, procesy a postupy potrebné na vykonávanie ustanovenia IS.D.OR.200.

f) Organizácia musí mať zavedený postup na zabezpečenie dostatočného počtu zamestnancov v službe na vykonávanie činností, na ktoré sa vzťahuje táto príloha.

g) Organizácia musí mať zavedený postup na zabezpečenie toho, aby zamestnanci uvedení v písmene f) mali potrebnú spôsobilosť na plnenie svojich úloh.

h) Organizácia musí mať zavedený postup na zabezpečenie toho, aby zamestnanci uznali povinnosti spojené s pridelenými rolami a úlohami.

i) Organizácia zabezpečí, aby bola náležite stanovená totožnosť a dôveryhodnosť pracovníkov, ktorí majú prístup k informačným systémom a údajom, na ktoré sa vzťahujú požiadavky tohto nariadenia.

IS.D.OR.245. Vedenie záznamov

a) Organizácia vedie záznamy o svojich činnostiach riadenia informačnej bezpečnosti.

1. Organizácia zabezpečí archiváciu a vysledovateľnosť týchto záznamov:

   i) každé prijaté schválenie a akékoľvek súvisiace posúdenie rizika v oblasti informačnej bezpečnosti v súlade s ustanovením IS.D.OR.200 písm. e);

   ii) zmluvy o činnostiach uvedených v ustanovení IS.D.OR.200 písm. a) bode 9;

   iii) záznamy o kľúčových procesoch uvedených v ustanovení IS.D.OR.200 písm. d);

   iv) záznamy o rizikách identifikovaných v posúdení rizika uvedenom v ustanovení IS.D.OR.205 spolu so súvisiacimi opatreniami na riešenie rizík uvedenými v ustanovení IS.D.OR.210;

   v) záznamy o incidentoch a zraniteľnostiach v oblasti informačnej bezpečnosti nahlásených v súlade so systémami nahlasovania uvedenými v ustanoveniach IS.D.OR.215 a IS.D.OR.230;

   vi) záznamy o tých udalostiach v oblasti informačnej bezpečnosti, ktoré možno bude potrebné prehodnotiť, aby sa odhalili nezistené incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti.

2. Záznamy uvedené v bode 1 podbode i) sa uchovávajú aspoň 5 rokov po uplynutí platnosti schválenia.

3. Záznamy uvedené v bode 1 podbode ii) sa uchovávajú aspoň 5 rokov po zmene alebo vypovedaní zmluvy.

4. Záznamy uvedené v bode 1 podbode iii), iv) a v) sa uchovávajú najmenej 5 rokov.

5. Záznamy uvedené v bode 1 podbode vi) sa uchovávajú dovtedy, kým sa uvedené udalosti v oblasti informačnej bezpečnosti opätovne neposúdia v súlade s periodicitou vymedzenou v postupe stanovenom organizáciou.

b) Organizácia vedie záznamy o kvalifikácii a skúsenostiach svojich vlastných zamestnancov zapojených do činností riadenia informačnej bezpečnosti.

1. Záznamy o kvalifikácii a skúsenostiach zamestnancov sa uchovávajú, pokiaľ daná osoba pracuje pre organizáciu, a najmenej 3 roky po tom, čo osoba opustila organizáciu.

2. Zamestnancom sa na ich žiadosť poskytne prístup k ich individuálnym záznamom. Okrem toho im organizácia na ich žiadosť poskytne kópiu individuálnych záznamov pri odchode z organizácie.

c) Formát týchto záznamov sa stanoví v postupoch organizácie.

d) Záznamy sa uchovávajú spôsobom, ktorým sa zabezpečí ochrana pred poškodením, pozmeňovaním a krádežou, pričom informácie sa v prípade potreby identifikujú na základe ich stupňa utajenia. Organizácia zabezpečí, aby sa záznamy uchovávali s použitím prostriedkov na zabezpečenie integrity, pravosti a oprávneného prístupu.

IS.D.OR.250. Príručka riadenia informačnej bezpečnosti (ISMM)

a) Organizácia sprístupní príslušnému orgánu príručku riadenia informačnej bezpečnosti (ISMM) a prípadne všetky súvisiace príručky a postupy, na ktoré sa odkazuje, obsahujúcu:

1. vyhlásenie podpísané zodpovedným manažérom alebo v prípade projekčných organizácií vedúcim projekčnej organizácie, ktorým sa potvrdzuje, že organizácia bude vždy pracovať v súlade s touto prílohou a s ISMM. Ak zodpovedný manažér alebo v prípade projekčných organizácií vedúci projekčnej organizácie nie je výkonným riaditeľom organizácie, potom vyhlásenie spolupodpíše takýto výkonný riaditeľ;
2. titul(-y), meno(-á), úlohy, zodpovednosť, povinnosti a právomoci osoby alebo osôb uvedených v ustanovení IS.D.OR.240 písm. b) a c);
3. prípadne titul, meno, úlohy, zodpovednosť, povinnosti a právomoci spoločnej zodpovednej osoby uvedenej v ustanovení IS.D.OR.240 písm. d);
4. politiku informačnej bezpečnosti organizácie, ako sa uvádza v ustanovení IS.D.OR.200 písm. a) bode 1;
5. všeobecný opis počtu a kategórie zamestnancov a zavedeného systému na plánovanie dostupnosti personálu, ako sa vyžaduje v ustanovení IS.D.OR.240;
6. titul(-y), meno(-á), úlohy, zodpovednosť, povinnosti a právomoci kľúčových osôb zodpovedných za vykonávanie ustanovenia IS.D.OR.200 vrátane osoby alebo osôb zodpovedných za funkciu monitorovania súladu uvedenú v ustanovení IS.D.OR.200 písm. a) bode 12;
7. organizačnú schému znázorňujúcu súvisiace reťazce zodpovednosti a povinností osôb uvedených v bodoch 2 a 6;
8. opis schémy interného nahlasovania uvedenej v ustanovení IS.D.OR.215;
9. postupy, ktoré špecifikujú, ako organizácia zabezpečuje súlad s touto časťou, a najmä:
   i) dokumentáciu podľa ustanovenia IS.D.OR.200 písm. c);
   ii) postupy, ktorými sa vymedzuje, ako organizácia kontroluje akékoľvek zazmluvnené činnosti uvedené v ustanovení IS.D.OR.200 písm. a) bode 9;
   iii) postup zmeny ISMM vymedzený v písmene c);
10. podrobné údaje o v súčasnosti schválenom náhradnom spôsobe dosiahnutia súladu.

b) Prvé vydanie ISMM schvaľuje a jej kópiu si ponechá príslušný orgán. ISMM sa podľa potreby zmení tak, aby bola naďalej aktuálnym opisom ISMS organizácie. Príslušnému orgánu sa poskytne kópia všetkých zmien ISMM.

c) Zmeny ISMM sa riadia postupom, ktorý stanovuje organizácia. Všetky zmeny, ktoré nepatria do rozsahu pôsobnosti tohto postupu, a akékoľvek zmeny týkajúce sa zmien uvedených v ustanovení IS.D.OR.255 písm. b) schvaľuje príslušný orgán.

d) Organizácia môže zlúčiť ISMM s inými príručkami riadenia alebo manuálmi, ktoré má k dispozícii, za predpokladu, že uvedie jasný odkaz označujúci časti príručky riadenia alebo manuálu, ktoré zodpovedajú rôznym požiadavkám obsiahnutým v tejto prílohe.

IS.D.OR.255. Zmeny systému riadenia informačnej bezpečnosti

a) Zmeny ISMS sa môžu riadiť a oznamovať príslušnému orgánu v rámci postupu, ktorý vypracuje organizácia. Tento postup musí schváliť príslušný orgán.

b) Pokiaľ ide o zmeny ISMS, na ktoré sa nevzťahuje postup uvedený v písmene a), organizácia musí požiadať o schválenie vydané príslušným orgánom a získať ho.

Pokiaľ ide o tieto zmeny:

1. žiadosť musí podať skôr, než uskutoční akúkoľvek takúto zmenu, aby sa príslušnému orgánu umožnilo stanoviť, či sa zachováva súlad s týmto nariadením, a v prípade potreby zmeniť osvedčenie organizácie a súvisiace podmienky schválenia, ktoré sú jeho prílohou;
2. organizácia musí sprístupniť príslušnému orgánu všetky informácie, ktoré si vyžiada na posúdenie zmeny;
3. zmena sa vykoná až po získaní formálneho schválenia od príslušného orgánu;
4. organizácia musí počas vykonávania takýchto zmien fungovať za podmienok predpísaných príslušným orgánom.

IS.D.OR.260. Neustále zlepšovanie

a) Organizácia s použitím primeraných ukazovateľov výkonnosti posúdi účinnosť a vyspelosť ISMS. Toto posúdenie sa vykonáva na základe harmonogramu, ktorý vopred stanoví organizácia, alebo v nadväznosti na incident v oblasti informačnej bezpečnosti.

b) Ak sa po posúdení vykonanom v súlade s písmenom a) zistia nedostatky, organizácia prijme potrebné opatrenia na zlepšenie s cieľom zabezpečiť, aby ISMS naďalej spĺňal príslušné požiadavky a udržiaval riziká v oblasti informačnej bezpečnosti na prijateľnej úrovni. Okrem toho organizácia opätovne posúdi tie prvky ISMS, ktorých sa týkajú prijaté opatrenia.