SIA BM CERTIFICATION GRUPAS

INFORMĀCIJAS UN INFORMĀCIJAS TEHNOLOĢIJU (IT) DROŠĪBAS POLITIKA

Informācijas un IT drošības politikas mērķis

SIA BM Certification (Uzņēmums) ir noteicis informācijas un IT drošības politiku (Politika), kuras mērķis ir paust Uzņēmuma vadības nostāju un atbalstu informācijas un IT drošības nodrošināšanai atbilstoši Uzņēmuma vajadzībām un interesēm, kā arī spēkā esošajam tiesiskajam regulējumam, kā arī nodrošināt uzņēmuma rīcībā esošās informācijas un tehnoloģisko resursu aizsardzību pret dažāda veida draudiem tā, lai draudu īstenošanās iespējamība (informācijas un IT drošības riski) būtu pieņemamā līmenī.

1. Uzņēmums nodrošina tādu IT vidi, lai tā rīcībā esošā informācija un tehniskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem un lai varētu savlaicīgi prognozēt un novērst šīs drošības apdraudējumu un tā radītās sekas.

2. Uzņēmuma vadība kopumā ir atbildīga par Politikas īstenošanu, t.sk. atbildīga par informācijas un IT drošības organizācijas izveidi un atbildības noteikšanu, IT ārpakalpojumu sniedzeja izvēli, kontroles noteikšanu un adekvātu resursu piešķiršanu informācijas un IT drošības pilnvērtīgai funkcionēšanai.

3. Saskaņā ar šo Politiku Uzņēmumā tiek noteikts un pastāvīgi tiek pilnveidots pasākumu kopums, kura īstenošana nodrošina drošības politikas mērķu sasniegšanu.

4. Uzņēmumā tiek nodrošināta pastāvīga drošības politikas īstenošanas koordinēšana un pārraudzīšana.

5. Uzņēmums nodrošina, ka tā rīcībā esošā informācija tiek pārvaldīta droši un vienoti.

6. Politika ir saistoša visiem Uzņēmuma darbiniekiem un arī ārpakalpojumu sniedzējiem.

7. Uzņēmumā tiek sekmēta katra darbinieka izpratne par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot Uzņēmuma darbinieku regulāru izglītošanu.

8. Risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Uzņēmuma darbības pārtraukšanas gadījumos.

9. Gadījumos, kad Uzņēmuma darbinieki neievēro Politikas prasības, Uzņēmuma vadība var ierosināt disciplinārās sodīšanas procesu saskaņā ar spēkā esošajiem normatīvajiem aktiem.

Informācijas un IT drošības politikas uzdevumi

Politikas galvenie uzdevumi ir:

1. nodrošināt informācijas pieejamību, t.i., tāda informācijas saglabāšana un uzturēšana, lai tā būtu pieejama īstajā laikā un īstajā vietā;

2. nodrošināt informācijas integritāti, t.i., informācijas veseluma, precizitātes un pareizuma nodrošināšana;

3. nodrošināt informācijas konfidencialitāti, t.i., informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot;

4. aizsargāt sistēmas informācijas resursus un tehniskos resursus, t.i., datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību;

5. noteikt sistēmas drošības apdraudējumu;

6. novērtēt sistēmas drošības risku;

7. atklāt sistēmas drošības incidentus;

8. atjaunot sistēmas darbību pēc sistēmas drošības incidenta.

Uzņēmums Politiku pārskata vismaz reizi gadā, kā arī gadījumos, ja izmaiņas sistēmā var ietekmēt sistēmas drošību, ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi vai ja pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents.

Politiku ir apstiprinājis SIA BM Certification izpilddirektors 2020. gada 3. septembrī

SIA „BM Certification"
Jūrkalnes iela 15, Rīga, LV- 1046, Latvija
T: +371 67772135
E: info@bmcertification.com
W: www.bmcertification.com