POLITIKA INFORMACIONE SIGURNOSTI

J.P.Međunarodni aerodrom „Sarajevo“ d.o.o. Sarajevo opredijeljeno je da:

- Uvjeri korisnike aerodromskih usluga i poslovne partnere da ćemo štititi sve informacije koje su nam dostavljene ili koje su kreirane u realizaciji naših usluga i poslovnih procesa;
- Osigura da su informacije zaštićene od neovlaštenog pristupa;
- Osigura povjerljivost i integritet informacija;
- Osigura dostupnost informacija ovlaštenim osobama i institucijama kada za to postoji obaveza;
- Vrši procjenu rizika po sigurnost informacija u planiranim intervalima i/ili kada se dese značajne promjene u organizaciji;
- Upravlja rizicima visokog ranga (high order risks) i svodi ih na prihvatljiv nivo kroz adekvatan plan za tretman rizika;
- Poštuje važeću legislativu i regulativu;
- Provodi obuke, gradi i održava svijest zaposlenika o značaju informacione sigurnosti;
- Osigura da su sve povrede informacijske sigurnosti prijavljene i istražene;
- Planira i provodi kontinuitet sigurnosti informacija kroz proces upravljanja kontinuitetom poslovanja;
- Zadovoljava zahtjeve ISO/IEC 27001:2013;
- Stalno poboljšava adekvatnost i efektivnost Sistema upravljanja sigurnošću informacija;
- Održava certifikaciju Sistema upravljanja sigurnošću informacija.

Sarajevo, 15.09.2016.

Direktor Društva
Armin Kajmaković

INFORMATION SECURITY POLICY

P.C. „SARAJEVO“ International Airport LLC Sarajevo has committed itself to the following:

- To convince users of airport services and business partners that all the information they sent us or those created during realization of our services and business relations;
- To secure the information from unauthorized access;
- To secure confidentiality and integrity of information;
- To enable available of information to authorized individuals and institutions when it is required;
- To make risk assessments related to security of information in regular intervals and/or in case of major organizational changes;
- To manage very high & high risks trying to reduce them to acceptable level using adequate plan for risk treatment;
- To comply with laws and regulatory rules being in force;
- To organize trainings, build up and sustain employees awareness on importance of the information security;
- To take care that all violations of the information security are reported and investigated;
- To plan and enable continuity of the information security through a process of managing the business continuity;
- To comply with ISO/IEC 27001:2013;
- To keep improving adequacy and effectiveness of the Information Security Management System;
- To maintain certification of the Information Security Management System.

Sarajevo, 15.09.2016.

Director
Armin Kajmaković