Gli operatori aeroportuali muniti di TIA sono tenuti al rispetto delle seguenti buone pratiche al fine di proteggere i sistemi fondamentali di tecnologia dell'informazione e comunicazione aeroportuali da potenziali attacchi informatici

1	Utilizzare i sistemi aeroportuali solo se adeguatamente formati ed istruiti
2	Non trasferire informazioni e dati dei sistemi aeroportuali, sia in formato elettronico che cartaceo, a soggetti che non hanno un legittimo motivo per accedere a tali sistemi
3	Utilizzare sempre la propria password personale per accedere ai sistemi aeroportuali, non comunicandola ad altri (ne lasciando tracce su post-it e bigliettini sulla postazione di lavoro) e avendo cura di attivare la modalità screen saver in caso di inattività prolungata
4	Non utilizzare un'unica password per accedere ai diversi sistemi aziendali e utilizzare password complesse (almeno 8 caratteri, almeno una lettera maiuscola, almeno un numero)
5	Comunicare al referente dei sistemi informatici della propria società eventuali tentativi di attacco informatico ricevuti (sia subiti che sventati)
6	Non cliccare su link o aprire allegati ricevuti via email di provenienza sospetta che possano condurre a siti malevoli
7	Diffidare da richieste via email, sms, telefono o sui social per richiesta di codici personali come password, codici di accesso ai servizi, PIN
8	Non collegarsi a reti Wi-Fi aperte / pubbliche non protette o differenti da quella predisposta dall'azienda
9	Non utilizzare pen-drive / memorie esterne se non esclusivamente predisposte dal personale IT
10	Non effettuare il download / installazione di software sui PC/dispositivi aziendali

Devono essere tempestivamente segnalate al Security Duty Officer di Ge.S.A.C. – tel.081/7896429/744 – anomalie che possano compromettere il corretto funzionamento dei sistemi aeroportuali, ad esempio:

- **Locali/Aree tecniche con PC/dispositivi dei sistemi aeroportuali non adeguatamente chiusi e non presidiati;**
- **Manomissione delle infrastrutture informatiche aeroportuali (lettori di badge, cavi rete, alimentazione ecc.);**
- **Tentativi di accessi non autorizzati alle attrezzature informatiche utilizzate per processare/conservare e trasmettere informazioni e dati (es. segni di manomissione su cavi Kensington, password bloccate per ripetuti log-in falliti);**
- **Ritrovamento di PC operativi (es. banchi check-in, gate ecc.) con cavi esterni collegati/pen-drive «sospette» inserite;**
- **Perdita/sottrazione di device aziendali/USB con dati sensibili (es. codici di accesso/credenziali e password) riconducibili ai sistemi aeroportuali;**
- **Ricezione di telefonate/email/messaggi di minaccia di un attacco informatico nei confronti dei sistemi e della rete informatica aziendale.**