Information Security Policy – VCY Travel AB

Organisationsnummer: 559477-3631

1. Syfte

Syftet med denna policy är att säkerställa skyddet av all information som hanteras av VCY Travel AB, inklusive kunddata, bokningar och betalinformation, samt att följa kraven enligt GDPR, IATA:s regler och GDS-leverantörer såsom Amadeus och Sabre.

2. Tillämpningsområde

Denna policy gäller alla anställda, partners och externa parter som hanterar eller får åtkomst till: kunduppgifter, bokningssystem (GDS), interna IT-resurser och IATA-relaterad information.

3. IATA:s säkerhetskrav

- PCI DSS: Betaluppgifter hanteras enligt PCI DSS.
- CRP: Incidentrapportering sker enligt IATA CRP.
- Endast auktoriserade anställda får åtkomst till IATA-portaler.
- Endast auktoriserade anställda får tillgång till finansiella rapport och BSP portalen.

4. Säkerhet i GDS: Amadeus

- Eget login + lösenord krävs.
- Multi-Factor Authentication (MFA) är obligatoriskt.
- PNR-data är konfidentiell och krypteras under överföring.
- Åtkomstloggar granskas regelbundet.

5. Säkerhet i GDS: Sabre

- Alla agenter har unika användarkonton + lösenord.
- API-åtkomst kräver godkända integrationer.
- Åtkomstloggar granskas regelbundet.

6. Teknisk säkerhet

- Kryptering, antivirus och VPN.
- Data lagras krypterad.
- Multi-Factor Authentication (MFA)
- Endast behöriga användare får åtkomst till system
- Alla enheter är utrustade med centralstyrt antivirus/antimalware som övervakar och rapporterar säkerhetsincidenter i realtid
- Passuppgifter raderas efter avslutad bokning. I undantagsfall kan uppgifterna lagras krypterat med kundens uttryckliga samtycke, exempelvis för att underlätta framtida resor.

7. Incidenthantering

- Incidenter rapporteras omedelbart.
- Vid personuppgiftsincident sker anmälan till IMY inom 72 timmar.

8. Utbildning

Alla anställda får GDPR- och GDS-utbildning vid anställning och årligen.

09. Databrottsförsäkring

VCY Travel AB är försäkrat mot databrott genom en särskild cybersäkerhetsförsäkring. Försäkringen omfattar följande skydd och proaktiva tjänster:

- Övervakning av läckta användaruppgifter i databasläckor
- Regelbunden webbside-besiktning för att identifiera sårbarheter
- Månadsbrev till anställda med tips och nyheter om informationssäkerhet
- Simulerade phishing-tester för att identifiera riskbeteenden

10. Revision

Denna policy uppdateras årligen eller vid större förändringar.