Version 1 2025-12-16
Uppdaterad version 2026-03-06

Informationssäkerhet

Lagring och dataöverföring

Informationen lagras i Sverige i en datahall som ägs av Västra Götalandsregionen. Någon överföring av personuppgifter utanför EU/EES förekommer inte.

Autentisering

- **webSolen:** Multifaktorautentisering (MFA) används.
- **Verksamhetsportalen:** Västtrafik arbetar för att införa tvåfaktorsautentisering i linje med webSolen.

Behörigheter

Systemen är behörighetsstyrda och använder personliga användarkonton. För **webSolen** finns ingen möjlighet till finfördelad behörighetsstyrning. Behörighet baseras på avtalet mellan Västtrafik och kommunen, och det är kommunens ansvar att endast ange användare som ska ha åtkomst.

Ledningssystem för informationssäkerhet

Västtrafik har ett ledningssystem för informationssäkerhet som motsvarar ISO 27001.

Kryptering

- **Kommunikation:** TLS 1.2 används som standard. TLS 1.3 stöds av operativsystem som har protokollet aktiverat som standard, exempelvis Windows Server 2022 och senare.
- **PKI:** En separat PKI-miljö finns.
- **Data i vila:**
    - Lagringslösningen är krypterad at-rest.
    - Databaser är som standard inte krypterade at-rest, även om vissa system använder detta.
    - VM-backuper är krypterade in-transit. Övriga backuper är krypterade at-rest.

Nyckelhantering

Certifikatnycklar lagras av mottagaren och/eller i lösenordsvalv. Nycklar för databaskryptering lagras separat från den krypterade informationen.

Backup och återställning

- **Frekvens:** Dagliga snapshots tas direkt på lagringslösningen. Dessutom finns ytterligare snapshots som lagras över längre tid via backup-programvara anpassad för virtuella miljöer.
- **Backupmetod:** Snapshots kompletterar traditionella backuper. Generellt tas backuper av hela den virtuella servern i stället för enskilda filer. För system där högre krav finns tas export i respektive systems proprietära format (t.ex. MSSQL).
- **Skydd:** Snapshots och backuper är immutabla och lagras i en separat datahall.
- **Återställning:** RTO är normalt högst 30 minuter från det att en backuptekniker påbörjar återläsningen.
- **RPO och lagringstid:**
    - RPO är vanligtvis 1 dygn, men kan vara några timmar för filservrar och e-post samt 15 minuter för MSSQL i produktion.
    - Standardlagringstid är 90 dagar, om inte systemägare beslutat annat.

Skydd mot skadlig kod och säkerhetstester

Västtrafik har skydd mot skadlig kod på samtliga klienter och servrar. Interna och externa sårbarhetsscanningar genomförs, liksom säkerhetstester baserat på riskbedömning.

Loggning

Loggning sker utifrån systemens behov och finns på flera nivåer, från infrastruktur till applikation. Både användar- och funktionsnivå kan loggas.

Gallring och radering

- Västtrafiks gallringsbeslut gäller för hantering av information.
- Radering enligt GDPR är möjlig så länge uppgifterna inte ingår i allmän handling. För allmänna handlingar styrs radering av Västtrafiks beslut om bevarande och gallring.
- Gallringsfrister varierar beroende på handling och kan innebära allt från omedelbar radering till bevarande för alltid.

Incidenthantering

Rutinerna varierar beroende på incidenttyp. Vid personuppgiftsincidenter där uppdragsgivaren är personuppgiftsansvarig rapporteras incidenter inom 48 timmar för att uppfylla 72-timmarsregeln.

Tillgänglighet (WCAG)

Nuvarande lösning uppfyller inte WCAG 2.0. För Boka Resa-appar och webblösningar arbetar Västtrafik för att uppnå WCAG 2.1 AA-nivå.

Personuppgiftshantering och systembehörigheter

Personuppgiftsbiträdesavtal

Västtrafiks PUB-avtal gäller för avtalet och är samma för samtliga uppdragsgivare.

Power BI

- Power BI används i lokala miljöer (on-prem).
- Ingen överföring av personuppgifter till tredje land sker.
- Åtkomst och loggning hanteras av IT-infrastruktur.
- Västtrafik gallrar historiska data enligt överenskommelse med verksamhetens informationscontroller.

Behörigheter i webSolen

Det går inte att göra ytterligare behörighetsbegränsningar i webSolen. Behörigheten bygger på att uppdraget hanteras som en helhet enligt avtalet mellan kommunen och Västtrafik. Kommunen ansvarar för att användare hanterar informationen korrekt.