Systembeskrivning - PortPoint

Version 3 september 2026 · portpoint.app/systembeskrivning

Det här dokumentet beskriver PortPoints arkitektur, säkerhetsåtgärder, personuppgiftshantering, drift och tillgänglighet. Det är avsett som bilaga till anbud och som underlag för leverantörsbedömning. Samma text finns på portpoint.app/systembeskrivning och uppdateras där när något ändras.

Tjänsten i korthet

PortPoint är en webbtjänst för gästhamnar, campingar och parkeringar. Gästen väljer anläggning och plats, betalar med Swish, kort, Apple Pay eller Google Pay och får kvittot i mobilen. Kvittot är biljetten: det visar platskod, giltighet och anläggningens koder till dusch, wifi och toaletter.

Anläggningens personal arbetar i PortAdmin: hamnkarta med zoner och platser, prislistor per båtlängd och säsong, förbokning med väntelista, digital kontrollrunda, kvitton, återbetalningar och statistik. Månads- och årsrapporter skapas automatiskt som PDF.

PortPoint är teknisk leverantör. Betalningarna går direkt från gästen till anläggningens egen Swish Handel-mottagare respektive Stripe-konto; PortPoint håller aldrig medel och har ingen tillgång till dem.

Arkitektur och driftmiljö

Applikationen är byggd i Next.js och körs på Cloudflare Workers via OpenNext, under domänen portpoint.app. Cloudflare terminerar TLS, sköter hastighetsbegränsning och levererar statiska resurser från sitt globala nät.

Databas (PostgreSQL), autentisering och fillagring tillhandahålls av Supabase. Projektet ligger i regionen Stockholm (AWS eu-north-1) - personuppgifter i vila lagras inom Sverige och EU.

Schemalagda jobb (rapporter, påminnelser, gallring, hälsolarm) körs av databasens egen schemaläggare (pg_cron) som anropar signerade adresser i applikationen. E-post skickas via Resend.

All källkod är versionshanterad i git. Varje driftsättning är versionerad hos Cloudflare och kan rullas tillbaka till en tidigare version på några minuter.

Datalagring och underbiträden

Personuppgifter lagras i Supabase-projektets databas och fillagring i Stockholm. Säkerhetskopior tas dagligen av Supabase i samma region.

Kartunderlag (satellitbild från Esri, kartdata från OpenStreetMap) och väderprognoser (SMHI) hämtas av besökarens webbläsare direkt från respektive tjänst. Dessa tjänster ser besökarens IP-adress men får inga uppgifter från PortPoint. Typsnitt byggs in i applikationen vid bygget - inga anrop till Google vid besök. PortPoint använder inga annons- eller spårningsskript och inga tredjepartskakor.

- Supabase Inc. - databas, autentisering och fillagring (Stockholm, AWS eu-north-1)
- Cloudflare Inc. - drift av applikationen, TLS, hastighetsbegränsning (globalt nät;

personuppgifter i vila lagras inte hos Cloudflare)
- Stripe Payments Europe Ltd. - kort, Apple Pay och Google Pay; kortuppgifter hanteras uteslutande av Stripe (PCI DSS)
- Getswish AB - Swish Handel; betalningen sker mellan gästens bank och anläggningens bank
- Resend Inc. - utskick av e-post (kvitton, notiser, larm)

Åtkomst, roller och autentisering

PortPoint har fem roller: superadmin (plattformen), hamnägare, hamnadministratör, användare och gäst. Rollen lagras i databasen - aldrig i klienten eller i en kaka - och varje tabell skyddas av radnivåsäkerhet (RLS) så att en användare bara kan läsa och ändra det rollen tillåter. Servernyckeln som går förbi RLS finns enbart på servern.

Hamnägaren ger sin personal tillgång per anläggning på nivån läsa eller redigera, och kan begränsa redigering till områden som priser, karta eller ekonomi. Personal bjuds in med engångslänk och kan tas bort på en minut. Varje ändring i PortAdmin loggas med vem, vad och när.

Lösenord kräver minst 8 tecken för gäster och användare och minst 12 tecken för alla PortAdmin-roller, med bokstäver och siffror. Vid val av lösenord kontrolleras det mot Have I Been Pwneds register över läckta lösenord med k-anonymitet - lösenordet lämnar aldrig servern. Lösenord lagras hashade (bcrypt) av Supabase Auth.

Tvåfaktorsautentisering (TOTP med återställningskoder) stöds för PortAdmin-konton. När den är aktiverad på ett konto krävs engångskoden vid varje inloggning i PortAdmin och systemadministrationen. Konton kan se sina aktiva enheter och logga ut enskilda sessioner; e-postbyte kräver verifiering med kod till den nya adressen.

Sessioner lagras i httpOnly-kakor som JavaScript i webbläsaren inte kommer åt. Administratörssessioner loggas ut automatiskt efter 28 timmars inaktivitet. Inloggning, lösenordsåterställning, betalstarter och öppna formulär är hastighetsbegränsade per IP-adress och konto.

Betalningar

Swish-betalningar går via Swish Handel med anläggningens eget avtal. PortPoint kommunicerar med Swish över ömsesidigt autentiserad TLS (klientcertifikat) och tar emot betalningsbeskedet; pengarna går mellan gästens och anläggningens banker.

Kort, Apple Pay och Google Pay hanteras av Stripe med anläggningens eget Stripe-konto. Kortuppgifterna matas in i Stripes egna komponenter och passerar aldrig PortPoints servrar. Stripe ansvarar för PCI DSS-efterlevnad. Swish kan även köras genom Stripe som alternativ väg.

Varje köp får ett kvitto med löpnummer, momsspecifikation per rad och säljarens (anläggningens) namn och organisationsnummer. Återbetalningar skapar kreditnota. Swish-avstämningar körs schemalagt och journalförs; köp som fastnat i väntande läge larmas i systemadministrationen.

Personuppgifter och GDPR

Anläggningen (hamnen, campingen, parkeringsägaren) är personuppgiftsansvarig för sina gästers uppgifter och PortPoint är personuppgiftsbiträde. Ett personuppgiftsbiträdesavtal

(PUB) tecknas med varje kund och registreras i systemet med version och signeringsdatum.

Uppgifter som behandlas: namn, e-postadress och telefonnummer, fordonsuppgifter (båtnamn, längd, registreringsnummer), köp- och betalningsreferenser samt tekniska loggar. Kortnummer lagras aldrig. Bevisfoton vid kontrollavgifter lagras i en privat lagringsyta som bara behörig personal når.

Lagringsminimering är inbyggd: anonyma gästkonton utan köp de senaste 30 dagarna raderas automatiskt, oanvända inbjudningslänkar och tillfälliga fordonsuppgifter gallras schemalagt, och köp som aldrig slutfördes rensas. Varje användare kan exportera sina uppgifter och radera sitt konto själv från profilsidan.

Alla åtgärder i PortAdmin skrivs till en händelselogg. Personuppgiftsincidenter dokumenteras i en incidentjournal oavsett om de anmäls; rör incidenten personuppgifter med risk för de registrerade anmäls den till Integritetsskyddsmyndigheten inom 72 timmar och berörd anläggning informeras utan dröjsmål.

Övervakning, säkerhetskopior och kontinuitet

Två oberoende övervakningslager: en extern upptidstjänst anropar hälsokontrollen /api/halsa, och ett internt jobb kör samma kontroll var 15:e minut och mejlar drift om en delkomponent (databas, betalning, e-post) inte svarar. Varje mätning sparas och ritar den publika statussidans 90-dagarshistorik på portpoint.app/status.

Supabase tar automatiska dagliga säkerhetskopior av databasen. Rutinen är att återställning testas till ett separat projekt minst en gång per kvartal och journalförs i systemadministrationen - en säkerhetskopia som aldrig testats räknas inte som en säkerhetskopia. Applikationskoden kan rullas tillbaka till valfri tidigare driftsättning.

Hemligheter (API-nycklar, certifikat, signeringsnycklar) lagras som krypterade secrets hos Cloudflare och finns aldrig i källkoden. Incidentrutinen följer fem steg: upptäck och bekräfta, begränsa, åtgärda och verifiera, kommunicera, dokumentera.

Ingen formell SLA-nivå ingår i standardvillkoren; drifthistoriken redovisas i stället öppet på statussidan. Servicenivåer kan avtalas i samband med upphandling.

Inget återställningstest är journalfört ännu.

Säkerhetsåtgärder i webbskiktet

Alla svar bär säkerhetsrubriker: Strict-Transport-Security i två år med preload, X-Frame-Options DENY och Content-Security-Policy frame-ancestors 'none' (applikationen kan inte bäddas in i andra sajter), X-Content-Type-Options nosniff och Referrer-Policy strict-origin-when-cross-origin. Permissions-Policy stänger av kamera och mikrofon och tillåter geolokalisering och betalning enbart där de behövs.

All indata valideras på servern oberoende av vad klienten skickat. Öppna formulär (demo- och mötesförfrågningar) har honungsfälla mot robotar och IP-gräns. Bilduppladdningar är begränsade i storlek och typ. Delbara länkar (biljetter, kvitton, recensioner) signeras med HMAC så att de inte kan gissas eller manipuleras.

Säkerhetsgranskningar dokumenteras i databasens migrationer med datum och åtgärd, så att varje förändring i behörighetsmodellen går att följa i efterhand.

Tillgänglighet

PortPoint arbetar mot lagen om tillgänglighet till digital offentlig service och WCAG 2.1 nivå AA. Tjänsten är delvis förenlig: sidorna fungerar med tangentbord och synligt fokus, respekterar inställningen för reducerad rörelse och stödjer förstoring samt ljust och mörkt läge.

Kända brister redovisas öppet i tillgänglighetsredogörelsen på portpoint.app/tillganglighet: de interaktiva kartorna är svåra att använda med skärmläsare (samma val går alltid att göra via sök, lista och textfält), och enstaka kontraster och PDF-kvitton når inte fullt ut AA. Den som inte kan använda en del av tjänsten får hjälp direkt - personalen kan registrera en betalning eller ta fram ett kvitto manuellt. Myndigheten för digital förvaltning (DIGG) utövar tillsyn.

Support och kontakt

Frågor, brister och önskemål tas emot via plattformens kontaktadress. Driftstatus kan alltid kontrolleras på portpoint.app/status utan inloggning. En klickbar demo av hela flödet - gästens betalning, kvittot och PortAdmin - finns på portpoint.app/demo, och utvärderare kan få en tidsbegränsad läsåtkomst till en testanläggning i den riktiga PortAdmin.

Kontakt	**portpoint.se@gmail.com**
Driftstatus	**portpoint.app/status**
Tillgänglighet	**portpoint.app/tillganglighet**
Säkerhet	**portpoint.app/sakerhet**