IT- og sikkerhetspolicy

Sport for Alle Norge AS Versjon 3.7 — Sist oppdatert: 5. mars 2026

Formål

Denne policyen beskriver hvordan ansatte i Sport for Alle Norge AS skal bruke IT-utstyr og digitale systemer på en trygg og forsvarlig måte. Brudd på policyen kan føre til advarsel, oppsigelse og i alvorlige tilfeller politianmeldelse.

IT-ansvarlig: Tor Pedersen, it@sportforalle.no, telefon 73 90 12 04.

1. Utstyr

Hva du får

Stilling	Standardutstyr
Kontor (admin/innkjøp/regnskap)	Bærbar PC (Dell Latitude eller MacBook), iPhone, Bluetooth-tastatur og mus
Butikk	Felles iPad ved kassen, ikke personlig PC
Lager	Felles PC på pakkestasjon, håndholdt skanner
Ledere	Bærbar PC + iPhone + iPad ved behov

Utstyr er bedriftens eiendom og leveres tilbake ved fratredelse.

Skadet eller mistet utstyr

Meld umiddelbart til IT (it@sportforalle.no) ved tap eller skade. For mistet eller stjålet telefon ringes IT eller daglig leder direkte for å sperre konti.

Forsikring dekker normal slitasje og uhell. Grov uaktsomhet kan medføre at du selv må dekke deler av kostnaden.

2. Passord og innlogging

Krav

- Passord skal være minst **14 tegn**
- Skal inneholde stor bokstav, liten bokstav, tall og spesialtegn
- Ikke gjenbruk passord på tvers av tjenester
- Bruk Bitwarden (vår passordmanager — alle ansatte får lisens)

Tofaktorautentisering (2FA / MFA)

Tofaktor er obligatorisk på følgende systemer:

- Microsoft 365 (e-post, OneDrive, SharePoint)
- Tripletex (lønn, utlegg)
- Visma eAccounting (regnskap)
- Shopify (nettbutikk-admin)
- Bitwarden
- VPN-tilgang

Bruk Microsoft Authenticator eller Bitwarden Authenticator. Aldri SMS-kode hvis app-basert kode er tilgjengelig.

Hvis du glemmer passord

Selvbetjent reset på passord.sportforalle.no, eller kontakt IT i åpningstid mandag–fredag 09–16.

3. E-post

Bruk

Bedriftens e-post er for arbeidsrelaterte formål. Begrenset privat bruk er greit, men:

- Ikke registrer bedriftens e-post for private tjenester (Spotify, sosiale medier, dating, etc.)
- Ikke videresend bedriftsinformasjon til private e-postkontoer

Phishing

Phishing er den vanligste angrepsvektoren mot bedriften vår. Vær årvåken!

Røde flagg:

- Uventet e-post med vedlegg eller lenke

- Hastesaker som krever umiddelbar handling ("logg inn nå eller kontoen sperres")
- Avsenderadresse som ligner men ikke er identisk (sportforalle.no vs. sportforalle.no — l vs. I)
- Forespørsler om å overføre penger eller endre kontonummer på leverandører

Ved mistanke: rapporter til it@sportforalle.no og slett. Ikke klikk på lenker eller åpne vedlegg.

Vi kjører phishing-simulering 4 ganger per år. Resultatene brukes til opplæring, ikke til straff.

Konfidensiell informasjon

Send aldri følgende på vanlig e-post:

- Personnummer eller fødselsnummer
- Passord
- Bankkontoinformasjon
- Kundedata i bulk

Bruk Microsoft 365 sin "kryptert e-post"-funksjon eller del lenker via OneDrive med tilgangskontroll.

4. Sikkerhet ved fjernarbeid

Hjemmekontor

- VPN (Cisco AnyConnect) skal alltid være på når du jobber utenfor kontoret
- Ikke jobb på offentlig WiFi uten VPN
- Lås PC-en når du forlater den, også hjemme

Privat utstyr (BYOD)

Bruk av privat utstyr (egen PC, mobil) til arbeidsformål er kun tillatt for:

- E-post via Outlook-app eller webmail
- Microsoft Teams
- Tilgang til OneDrive-filer

For utvikling, regnskap og admin-tilgang skal du bruke arbeidsgivers utstyr. Se IT-sjefen ved spesielle behov.

5. Datalagring

Hvor lagres hva?

Type data	Lagringssted
Pågående arbeid (dokumenter, regneark)	OneDrive (din personlige)
Felles avdelingsdokumenter	SharePoint (avdelingsmappen)
Kundedata	Shopify (varehandel) + Visma (regnskap)
Personalopplysninger	Tripletex
Backup av lokalt arbeid	Automatisk OneDrive-sync

Lagre **aldri** arbeidsfiler kun lokalt på maskinen — de er ikke beskyttet av backup.

USB-pinner og eksterne disker

Bruk av USB-pinner er tillatt, men:

- USB-pinnen må være kryptert (BitLocker eller Apple FileVault)
- Eksterne harddisker må registreres hos IT
- Ikke koble til ukjente USB-enheter (gratis-enheter på messer, mistet på gata, etc.)

6. Programvare

Tillatt

Bruk kun programvare som er forhåndsgodkjent og installert via Intune (PC-distribusjonsplatformen). Standardliste finnes på intranettet.

Skyløsninger

Før du tar i bruk en ny skytjeneste (selv om den er gratis), avklar med IT. Vi må vurdere om den oppfyller GDPR-krav og om databehandleravtale trengs.

Tjenester som krever vurdering: alt der du laster opp bedriftsdata (Notion, Trello, Figma, ChatGPT, Claude, Google Drive privat, Dropbox, etc.).

For AI-verktøy: vi bruker **Microsoft Copilot for Business** (kommer Q2 2026) som godkjent løsning. Inntil videre kan du bruke Claude eller ChatGPT med to begrensninger: (a) ikke last

opp kundedata eller intern strategi, (b) ikke aktiver chatlagring/historikk.

Personlig programvare

Det er ikke tillatt å installere personlig programvare på bedriftens utstyr (spill, torrent-klienter, kryptovaluta-mining, hacking-verktøy).

7. Sosiale medier

Du er fritt å være aktiv på sosiale medier i fritiden. Hvis du nevner Sport for Alle som arbeidsgiver i biografien, husk:

- Skill mellom personlige meninger og bedriftens posisjon
- Ikke del intern informasjon (priser, leverandører, ansattforhold) offentlig
- Vær respektfull i tone, særlig overfor kunder og konkurrenter

Markedsavdelingen håndterer offisielle kanaler (Instagram, Facebook, TikTok). Ikke poste på vegne av bedriften uten avtale.

8. Når du slutter

Senest siste arbeidsdag:

- Lever inn alt utstyr (PC, telefon, nøkler, adgangskort)
- Tilganger sperres av IT samme dag
- Personlige data på OneDrive må du ha kopiert ut selv på forhånd
- Bedriftsdata på private enheter skal slettes (du får hjelp av IT)

9. Sikkerhetshendelser

Ved mistanke om sikkerhetshendelse (innbrudd på konto, hacking, ransomware-melding) varsle IT umiddelbart, telefon eller SMS til Tor Pedersen (902 11 234) — også på kveld og helg.

10. Brudd på policy

Brudd kan medføre:

- Muntlig advarsel
- Skriftlig advarsel

- Inndragning av tilganger
- Oppsigelse
- Politianmeldelse ved straffbare forhold (ID-tyveri, datainnbrudd)