1.2. Kirjautuminen Netvisor KYC:iin

Netvisor KYCin käyttäjätunnus on henkilökohtainen ja käyttäjä on vastuussa omilla tunnuksillaan palvelussa tehdyistä toimenpiteistä. Netvisor-palvelun kirjautuminen tapahtuu aina vahvalla 2FA-tunnistautumisella. Saatavilla olevat kirjautumistavat ovat:

- Käyttäjätunnukseen, salasanaan ja tekstiviestitse toimitettavaan kertakäyttöiseen koodiin pohjautuva tunnistautuminen
- Microsoft Entra ID -pohjainen AD-kirjautuminen

Palvelun käyttö ei ole mahdollista pelkällä käyttäjätunnus-salasana -yhdistelmällä. Yksittäisiä palvelun osia on mahdollista päästä käyttämään suoraa linkillä, jonka kautta palveluun siirtyessä käyttäjälle lähetetään kertakäyttöinen tunnistuskoodi tekstiviestillä tai sähköpostilla. Tämän kautta kuitenkin voi palvelussa tehdä vain ennalta määriteltyjä toimenpiteitä (kuten tietopyyntöön vastaaminen).

1.3. Integraatiot

Netvisor KYC-palvelu on yhdistetty useisiin kolmannen osapuolen palveluihin, jotka tarjoavat käyttäjille automaatiota ja lisäominaisuuksia.

- Integraatiot Netvisor KYC:stä esimerkiksi projektinhallintasovelluksiin
- Asiakkaiden omat integraatiot heidän ERP-järjestelmästä Netvisor KYC -sovellukseen.

Sisäänrakennettujen integraatioiden lisäksi Netvisor KYC tarjoaa integraatiokumppaneiden käyttöön ohjelmistorajapinnan, jonka avulla järjestelmään voidaan liittää kolmansien osapuolien ohjelmistoja. Kaikki rajapintaliikenne on valvottua ja suojattua. Käyttäjä voi milloin tahansa katkaista integraation omiin tietoihinsa verkkopalvelun kautta.

Ajantasainen lista integraatioista eri palveluihin löytyy Netvisor KYC:n sivuilta.

1.4. Mitä pakotelistoja Netvisor KYC käyttää pakotelistavertailussa

Netvisor KYC -palvelu hyödyntää pakotelistavertailussa aina ajantasaisinta saatavilla olevaa tietoa. Palvelu käyttää virallisia pakotelistoja varmistaakseen luotettavan ja ajankohtaisen seulonnan. Käytettävät listat sisältävät Yhdistyneiden Kansakuntien (YK) pakotelistan, Ison-Britannian (UK) listan, Euroopan unionin (EU) pakotelistan, Yhdysvaltojen OFAC-listan (Office of Foreign Assets Control), Kanadan hallituksen pakotelistan sekä Keskusrikospoliisin (KPR) ylläpitämän varainjäädytyslistan. Näin varmistetaan, että tunnistetut henkilöt ja organisaatiot tarkastetaan kattavasti kansainvälisiä vaatimuksia vasten.

Nimien vertailu pakotelistoihin tehdään hyödyntämällä yleisesti hyväksyttyjä vertailualgoritmeja ja niiden yhdistelmiä. Näihin kuuluvat muun muassa merkkijonojen samankaltaisuutta arvioivat algoritmit, kuten fuzzy matching. Näin varmistetaan, että vertailu on sekä tarkka että joustava, ja että mahdolliset osumat tunnistetaan myös tilanteissa, joissa nimi esiintyy eri muodoissa tai kirjoitusasuissa.

2. Netvisor KYC:n tietoturva

Netvisor KYCin tietoturva pohjautuu Visma-konsernin omaan tietoturvaohjelmaan (Visma Security Program), jota kaikki Visman tuotteet noudattavat. Kyseisessä ohjelmassa Visman tuotteita tarkastellaan monesta eri näkökulmasta sekä automaattisten että manuaalisten tarkastusten kautta ja jokaisen tuotteen tietoturvasta on tiedossa reaaliaikainen tilannekuva.

2.1. Tekninen tietoturva

Palvelun osista ja sen toiminnasta vastuussa ovat Netvisor KYC tuotekehitystiimi.

Netvisor KYCin tekninen tietoturva on rakennettu kerroksittain ja eri osa-alueilla tietoturva on huomioitu käyttäen yleisesti suositeltuja käytäntöjä. Turvallinen tiedonsiirto käyttäjien ja Netvisor KYCin välillä sekä palvelun sisäisesti noudattaa mm. seuraavia periaatteita:

- Tiedonsiirto tehdään salattujen yhteyksien yli (encrypted data in transit)
- Palveluun tallennetut tiedot ovat salattu (encrypted data at rest)
- Pääsynhallinta järjestelmässä perustuu monikerroksiseen autentikaatioon sekä roolipohjaisuuteen (RBAC)
- Palvelinympäristön verkkoinfrastruktuuri on rakennettu alan hyvien käytäntöjen mukaisesti ja tietoturvastandardeja noudattaen

Osana Netvisor KYCin teknistä tietoturvaa palvelusta tuotetaan logitietoja käyttäjien toimista. Lokia analysoidaan sekä automaattisten hälytysten pohjalta, että manuaalisesti tasaisin väliajoin virhetilanteiden havaitsemiseksi. Analyysia tehdään vain palvelun tietoturvan takaamiseksi.

Palvelinympäristöissä käytetyt ohjelmistot (käyttöjärjestelmä, antivirusohjelmistot, muut palvelun tuottamiseen tarvittavat ohjelmistot) päivitetään säännöllisesti ja mahdollisiin tietoturvahaavoittuvuuksiin näissä ohjelmistoissa reagoidaan viipymättä. Sovellustasolla Netvisor KYC-palvelua kehitetään tietoturvaperiaatteet edellä, huomioiden muun muassa OWASP top 10 -uhat.

Käytössämme on myös automaattisia skannaustoimintoja, joiden avulla pyrimme havaitsemaan ja korjaamaan mahdolliset uhat mahdollisimman pian. Palvelun toimintaa tarkastellaan useasta näkökulmasta hyödyntäen alan parhaita työkaluja (SAST, SCA, DAST).

2.2. Hallinnollinen tietoturva

Netvisor KYC-palvelun hallinnollinen tietoturva pohjautuu Visma-konsernin omaan tietoturvaohjelmaan, joka on kaikille Visman tuotteille pakollinen. Visman tietoturvaohjelma käsittää jatkuvia tietoturvamittareita, sisäisiä tietoturva-auditointeja sekä hallinnollisten prosessien säännöllisiä tarkastuksia. Näistä osa-alueista koostuu jokaiselle Visma-tuotteelle oma Security Maturity Index, joka antaa reaaliaikaisen kuvan siitä, mikä kunkin Visma-tuotteen tietoturvan taso on. Lisätietoa Visman tietoturvaohjelmasta löytyy Visma Trust Centrestä.

Kaikki Visman työntekijät ovat velvoitettuja suorittamaan säännöllisesti konsernin tietoturva- ja tietosuojakoulutukset. Kaikkien Visman työntekijöiden sekä yhteistyökumppaneiden kanssa on solmittu salassapitosopimukset.

Vismalla on konsernitasoinen Responsible Disclosure-ohjelma, jonka kautta kuka tahansa voi luottamuksellisesti välittää Vismalle tiedon mahdollisesta haavoittuvuudesta missä tahansa Visman tuotteessa tai palvelussa.