Tietoturvakuvaus Webropol-kyselypalvelut

Tämä dokumentti sisältää yleiskuvauksen Webropol Survey & Reporting kysely-, raportointi- ja analyysityökalun tietoturvasta sekä tietosuojasta. Dokumentissa kuvataan yleisimpien tietoturvaan, tietosuojaan ja järjestelmien tekniseen tietoturvaan liittyvien kysymysten ratkaisut.

Heinäkuu 2026

Sisällysluettelo

Webropolista 3
Tietoturvan merkitys kyselypalvelua valittaessa 3
Tietoturva 3
Miten Webropol toimii? 4
Tietokannan kryptaus 5
Kerätty tieto 5
Lokitiedot ja kirjausketjut 6
Turvallinen tuotekehitys 6
Ote penetraatio- ja auditointilausunnosta 7
Fyysinen tietoturva 7
IPS-ominaisuus Webropolin palomuurissa 8
Kehittyneiden tietoturvauhkien havaitseminen 8
Häiriötilanteista palautuminen ja tiedon varmistus 8
IP-osoitteiden säilyminen 8
Euroopan Unionin säätely ja GDPR 9

Webropolista

Vuonna 2002 perustettu Webropol Oy on Webropol Survey&Reporting kysely- ja raportointisovelluksen kehittäjä. Palvelukokonaisuuten sisältyy kyselytyökalun lisäksi laaja valikoima lisämoduuleja sekä integraatioratkaisuja. Tarjoamme myös palveluita kuten koulutusta, konsultointia ja projektinhallintaa parhaan lopputuloksen saavuttamiseksi ratkaisujemme avulla. Tällä hetkellä meillä on toimipisteet Iso-Britanniassa, Saksassa, Ruotsissa ja Suomessa. Itsenäinen Webropol- jälleenmyyjä toimii Belgiassa. Webropol on kasvanut 20 vuoden aikana selvästi kansainväliseksi yritykseksi. Webropol-tytäryritykset ja - jälleenmyyjät ovat laajentaneet asiakaspohjamme jo 30 maahan.

Joka vuosi yli 14 miljoonaa ihmistä vastaa kyselytutkimuksiin, joita laatii kaikkiaan 70 000 Webropol-käyttäjää. Me pyrimme antamaan asiakkaillemme mahdollisimman täydellisen käyttäjä- ja asiakaskokemuksen. Kehitämme tuotetta jatkuvasti, jotta se pysyy helppokäyttöisenä ja erittäin tietoturvallisena. Haluamme tarjota asiakkaillemme vain parasta. Me uskomme kustannustehokkaaseen järjestelmään, jonka laadusta ja tietoturvasta ei tingitä.

Tietoturvan merkitys kyselypalvelua valittaessa

Verkkokyselyillä voit helposti ja nopeasti kerätä tietoa erilaisiin liiketoimintatarpeisiin. Vaikka tiedonkeruu onkin nykyään todella helppoa, on silti tärkeää muistaa tietoturvan ja tietosuojan merkitys. Kerätessäsi tietoa, erityisesti jos se sisältää henkilötietoja tai luottamuksellista liiketoimintaa koskevaa tietoa, on varmistuttava siitä, että sitä käsitellään asiankuuluvalla luottamuksellisuudella. Lisäksi on huomioitava tietoturvaa ja tietosuojaa koskeva lainsäädäntö ja muu mahdollinen säätely. Tämä koskee sekä kyselypalvelun käyttäjää että palveluntarjoajaa. Me Webropolilla otamme tietoturvaa ja tietosuojaa koskevat asiat erittäin vakavasti.

Tietoturva

Webropol on sitoutunut käyttämään alan parhaita teknisiä käytänteitä turvatakseen tietosi Webropol-palvelussa. Näillä menetelmillä ja prosesseilla varmistamme, että tietosi luottamuksellisuus on turvattu eikä luvaton käyttö ole mahdollista.

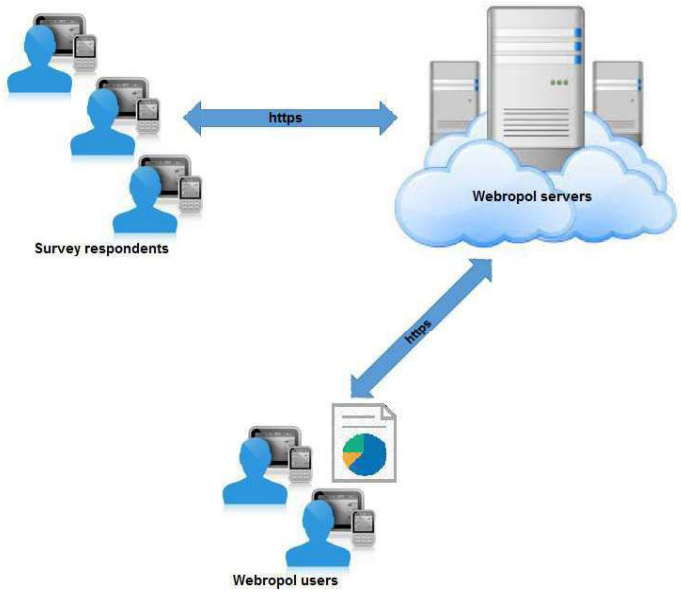
Webropol arvioi ja kehittää jatkuvasti loogista, organisaatiollista ja fyysistä tietoturvaansa. Tällä hetkellä teemme töitä saadaksemme käyttöön uusia ohjeistuksia ja käytäntöjä koskien niin teknisiä, fyysisiä ja organisaatiollista tietoturvaa. Webropol toiminta- ja toimistoympäristöllä (ICT-infrastruktuuri, tukipalvelut ja henkilöstö) on ISO 27001-sertifikaatti. Alihankkijamme, joka vastaa palveliemme ylläpidosta, on sertifioitu ISO 27001 standardin mukaan.

Webropol on tehnyt jatkuvaa, kuukausittaista yhteistyötä toistakymmentä vuotta tietoturva-alan huippuasiantuntijayritysten kanssa. Tällä hetkellä yhteistyökumppanimme on Prosecom Oy. Yhteistyöhön kuuluu lähdekoodin arviointi sekä palvelumme penetraatiotestit ja auditoinnit. Webropol käyttää Prosecom Oy:n konsultteja ohjelman tietoturvan testaamiseen. Testeistä saadun tiedon pohjalta voimme kehittää ympäristömme tietoturvaa ja hallita mahdollisia riskejä.

Miten Webropol toimii?

Webropol-palvelu tarjotaan asiakkaillemme SaaS- palveluna (Software as a Service). Palvelut koostuvat useista erillisistä web-sovelluksista sekä niitä tukevista taustapalveluista. Kaikki Webropolin käyttäjät ovat samassa SaaS -ympäristössä, mutta kaikki asiakasdata on rajattu erillisiin, loogisiin asiakasympäristöihin.

Webropolin käyttäjät luovat kyselyitä Webropol-alustalla osoitteessa: https://new.webropolsurveys.com. Verkkokyselyitä voi lähettää esimerkiksi sähköpostitse tai SMS-kutsuin, tai julkaisemalla linkin esimerkiksi kotisivuilla. Kun tietoa on kerätty, voivat käyttäjät luoda monipuolisen raportointi- ja analyysityökalun avulla visuaalisia raportteja, jakaa niitä tai tallentaa aineiston jossakin useista tuetuista tiedostomuodoista. Lisäksi kerättyä tietoa voi analysoida monipuolisella Webropol AI Tekstianalyysi -työkalulla tai Webropol Insights -työkalulla tehtävät ennusteanalyysit ja simulaatiot.



Kaikki palvelinten ja käyttäjien selaimen välinen liikenne on salattua,käyttäen TLS 1.2 ja TLS 1.3 salausalgoritmejä. Estettyjä versioita: TLS 1.0,TLS 1.1 sekä SSL 3.0.

Tietokannan kryptaus

Tietokanta on krypattu Microsoftin TDE-salauksella.

Kerätty tieto

Vaikka onkin tärkeää ymmärtää, miten Webropol toteuttaa kerätyn tiedon turvallisen käsittelyn, on myös yhtä lailla tärkeää tiedostaa, että kyselyn kysymysten laatiminen ja päätökset siitä, mitä tietoa kerätään, ovat aina Webropolia käyttävän asiakkaan vastuulla. Palvelulla kerätyn tiedon omistaa asiakas, ja asiakkaan on ymmärrettävä, että tiedosta voi muodostua asiakkaan vastuulla oleva henkilörekisteri. Jos kyselyaineisto sisältää henkilötietoja, on asiakkaan huomioitava henkilötietoja koskeva lainsäädäntö.

Palveluun kerättyä tietoa säilytetään oletusarvoisesti 1 kuukausi siitä hetkestä, kun käyttäjä käyttöliittymän kautta poistaa tiedon itse. Tarvittaessa vahingossa poistettu tieto voidaan palauttaa. Kaikki asiakkaan tiedot poistetaan 1 kuukauden kuluttua asiakkaan palvelusopimuksen päättymisestä.

Edellä kuvatun kyselytiedon lisäksi Webropol kerää ainoastaan eräitä käyttäjiin, ja teknisiin logeihin liittyviä tietoja. Lisätietoja kerättävistä tiedoista löytyy käyttöstatistiikkaan Tietosuojalain (5.12.2018/1050) mukaisesta rekisteriselosteesta.

Webropol on tehnyt tietoturvavaltuutetulle toimintailmoituksen: Dnro 1343/428/11.

Pääkäyttäjä voi luoda Webropoliin rajattoman määrän käyttäjätunnuksia yhteen asiakasympäristöön. Käyttäjätunnuksia on kahdentasoisia: Pääkäyttäjä ja Perustaso. Pääkäyttäjät voivat luoda uusia käyttäjätunnuksia asiakasympäristöön ja he hallinnoivat asiakkaan ympäristöä. Pääkäyttäjillä on pääsy kaikkiin kyselyihin ja raportteihin asiakkaan ympäristössä. Perustasoiset käyttäjät pääsevät niihin kyselyihin, jotka he ovat itse luoneet tai joihin heille on annettu pääsy, mutta eivät voi luoda muita käyttäjiä tai muuttaa käyttöympäristön yleisiä asetuksia. Pääsyoikeuksia voi antaa kolmella tasolla: **Lukuoikeus:** pääsee näkemään kyselyt ja raportit, mutta ei voi tehdä muutoksia **Kirjoitusoikeus:** pääsee näkemään ja muokkaamaan kyselyitä ja raportteja. Ei voi muokata kyselyn pääsyoikeuksia eikä poistaa kyselyä. **Hallintaoikeus:** voi tehdä kaikkia toimenpiteitä kyselylle. Vastaa kyselyn luojan oikeuksia.

Käyttäjätunnuksiin on liitetty sähköpostiosoite ja ne on suojattu käyttäjän itse valitsemalla salasanalla. Käyttäjien salasanat on tallennettu alan standardien mukaisesti SHA1- tiivisteinä (salted hash format). Webropolissa on mahdollista käyttää SAML 2.0/ADFS - pohjaista kertakirjautumisratkaisua (Single Sign-On, SSO). Webropolissa on suojaus ns. Brute Force -hyökkäystä vastaan: käyttäjätunnus lukkiutuu viiden epäonnistuneen kirjautumisyrityksen jälkeen.

Webropol suosittelee rajaamaan pääkäyttäjätasoiset oikeudet pienelle määrälle organisaation luotettuja käyttäjiä noudattaaksenne pääsynhallinnan prosessejanne. Suositeltavaa on kuitenkin nimetä vähintään kaksi pääkäyttäjää, jotta käytössä on myös varahenkilö varsinaisen pääkäyttäjän ollessa tavoittamattomissa.

Nimetyillä Webropolin asiakastuen henkilöillä on - asiakkaan kirjallisella luvalla - pääsy asiakkaan kyselyihin asiakastuen ja käytönneuvonnan antamiseksi. Webropolilla on tiukat politiikat ja kontrollit sen varmistamiseksi, ettei asiakasdataan päästä luvattomasti.

Lokitiedot ja kirjausketjut

Webropol-palvelut keräävät kattavasti lokitietoja ja kirjausketjuja (Audit Trail Log). Lokiin kirjataan tiedot esimerkiksi epäonnistuneista ja onnistuneista sisään- ja uloskirjautumisista, kyselytiedon lukemisesta, raportin tallentamisesta ulkoiseen tiedostomuotoon sekä käyttäjätunnusten ja pääsyoikeuksien luomisesta ja muokkaamisesta. Webropol Survey&Reporting -palvelussa lokien läpinäkyvyyttä on parannettu entisestään, muun muassa niin, että yksittäisten kyselyiden laatijat näkevät suoraan kyselyn tiedoista siihen kohdistuvat lokimerkinnät, esimerkiksi nähdäkseen onko joku muu käyttäjä katsonut raporttia.

Käyttäjien sisäänkirjautumistietoja säilytetään 10 vuotta. Tähän tietoon ei ole pääsyä muilla kuin Webropolin teknisellä tiimillä, emmekä luovuta tietoja eteenpäin kenellekään, edes kyselyn laatijalle.

Turvallinen tuotekehitys

Tietoturva on varmistettu tuotekehityksessä, käyttämällä tietoturva-alan parhaita käytänteitä sekä turvallisen tuotekehityksen standardeja. Webropol on tehnyt tuotekehityksen osalta jatkuvaa, kuukausittaista yhteistyötä toistakymmentä vuotta tietoturva-alan huippuasiantuntijayritysten kanssa. Tällä hetkellä yhteistyökumppanina on Prosecom Oy. Yhteistyöhon kuuluu lähdekoodin arviointi sekä palvelumme penetraatiotestit ja auditoinnit. Webropol käyttää Cyber Security Services -konsultteja ohjelman tietoturvan testaamiseen. Testeistä saadun tiedon pohjalta voimme kehittää ympäristömme tietoturvaa ja hallita mahdollisia riskejä.

Ote penetraatio- ja auditointilausunnosta

Information Security Statement

A security assessment was conducted by Prosecom Oy over a two-week period, which were performed to evaluate and ensure the integrity and security of the production environment lifecycle.
At Webropol Oy, the security of their web application and client data is treated as a critical priority. To uphold security standards, Webropol conducts quarterly security assessments to align with OWASP guidelines. These regular assessments target potential vulnerabilities within their staging environment, ensuring continuous and proactive risk mitigation.

Additionally, Webropol carries out comprehensive annual security audits on their production environment. These audits include evaluations of server configurations, firewall settings, vulnerability scanning, server hardening, and detailed technical reviews and interviews.
Any vulnerabilities identified during assessments are prioritized by Webropol for immediate resolution. Their developers participate in annual training specifically designed to reinforce secure coding practices, enhancing the security foundation of their applications.

Further security assessments are promptly conducted whenever significant changes are introduced to systems or applications, demonstrating Webropol's ongoing dedication to maintaining and continuously improving their security posture.

Through these proactive measures, Webropol consistently seeks to reinforcing customer trust by diligently addressing security risks and protecting client data.

Prosecom Oy
5.4.2025

Fyysinen tietoturva

Webropolin palvelimet sijaitsevat Telia Cygate Oy:n korkean tietoturvatason palvelinkeskuksissa Helsingissä. Palvelinkeskuksissa on kahdennetut varavirtalähteet, palosammutusjärjestelmä, tallentava kulunvalvonta ja anti-masking videovalvonta sekä 24/7/365 miehitetty valvonta.

Kaikki kriittiset komponentit (palvelimet, verkko, tallennusjärjestelmät) on kahdennettu erillisiin konesaleihin jatkuvan saatavuuden varmistamiseksi myös tilanteissa, jolloin verkossa tai muussa fyysisessä infrastruktuurissa on häiriötilanteita (Tier 3). Palvelinten hosting-palvelu sekä palvelinkeskukset auditoidaan säännöllisesti ja ne täyttävät esimerkiksi PCIDSS sekä Cloud Security Alliance v3 -vaatimukset.

IPS-ominaisuus Webropolin palomuurissa

IPS (Intruson prevention system) on palomuurin lisäominaisuus josta käytetään myös termiä murron estämisjärjestelmä. Järjestelmä pyrkii ottamaan kiinni vääränkaltaista liikennettä.
IPS:n avulla on mahdollista tunnistaa hyökkäyksiä, ja antaa ennalta määriteltyjä toimintoja näihin. Hyökkäys voi olla esimerkiksi sellainen, jossa yritetään järjestelmällisesti kokeilemalla löytää oikea salasana.
Tällä tavalla voidaan saada kiinni mm. ns. brute force ja 0-päivä hyökkäyksiä.

Tietokanta

Tietokanta on Webropolin omalla palvelimella Telia Cygaten korkean tietoturvatason palvelinkeskuksessa.

Kehittyneiden tietoturvauhkien havaitseminen

Webropolilla on käytössä Telia Cygaten palvelu: **Managed Detection and Response** (MDR). MDR:n tarkoituksena on havaita kehittyneitä tietoturvauhkia ja kohdistettuja hyökkäyksiä. Webropolin palvelimiin asennetun **Endpoint Detection and Respondent** (EDR) avulla arvioidaan palvelun hallintakäyttöliittymän tietojen perusteella havaitut tietoturvauhkat, analysoidaan ja tehdään tarvittavat toimenpiteet.

Palvelinalustan haavoittuvuusskannaukset ajetaan joka kuukausi Webropol-palvelussa käytettäviin palvelimiin.

Häiriötilanteista palautuminen ja tiedon varmistus

Webropol-palveluiden sisältämät tiedot varmuuskopioidaan päivittäin erilliseen, ammattilaistason varmistusjärjestelmään. Varmuuskopioita ei tehdä siirrettäville medioille tietoturvasyistä. Varmuuskopioita säilytetään 14 päivää. Webropolilla on erillinen jatkuvuus- ja häiriötilannesuunnitelma, jota testataan vuosittain.

IP-osoitteiden säilyminen

Kyselyn vastaajien IP-osoitteet säilyvät web-palvelimen lokissa kaksi (2) viikkoa. Tähän tietoon ei ole pääsyä muilla kuin Webropolin teknisellä tiimillä, emmekä luovuta tietoja eteenpäin kenellekään, edes kyselyn laatijalle.

VPN-yhteys

Webropolin tietoliikenne eri toimipisteiden ja palvelun tuottamiseen osallistuvien työntekijöiden etätyölaitteistoiden VPN-yhteys täyttää tietoturvaluokka TL III -tason vaatimukset.

Euroopan Unionin säätely ja GDPR

Webropol noudattaa toiminnassaan Suomen lainsäädäntöä. Euroopan Unionin jäsenmaana, EU-säädökset on huomioitu. Kaikki palvelun sisältämä tieto on tallennettu EU:n sisällä, eikä sitä missään tilanteessa luovuteta tai käsitellä EU:n ulkopuolella.

Euroopan Unionin yleisen tietosuoja-asetuksen (General Data Protection Regulation, GDPR) soveltaminen alkaa 28.5.2018, mikä yhtenäistää henkilötietojen käsittelyn koko Unionin alueella. Webropol on sitoutunut varmistamaan, että palveluidemme käyttö on asetuksen mukaista ja on kehittänyt palveluun toimintoja, jotka edesauttavat asiakkaidemme toimintaa asetuksen vaatimusten mukaisesti.

Webropol Oy Huovitie 3, 00400 Helsinki, Finland, www.webropol.fi

Lopuksi

Webropol käyttää alan parhaita teknologioita ja käytänteitä suojaamaan asiakkaidemme tietoa luvattomalta käytöltä. Nämä suojaavat toimenpiteet mahdollistavat asiakkaidemme käyttää Webropol-palvelua turvallisella tavalla, taaten kerätyn tiedon saatavuuden, eheyden ja luottamuksellisuuden.

Lisätietoja

Mikäli sinulla on kysymyksiä tai haluat lisää tietoa, ole hyvä ja ota yhteyttä sähköpostitse: servicedesk@webropol.com tai soittamalla paikalliseen Webropol -toimistoon:

Suomi: +358 20 155 2174
Ruotsi: +46 13 470 72 00
UK: +44 1788 833 881
Belgia: +32 2 808 04 30
Saksa: +49 202 94658630

Webropol Oy, Huovitie 3, 00400 Helsinki, Finland www.webropol.fi

Liite 1, OWASP-kuvaus

Tämä on kuvaus siitä, miten vältetään vähintään OWASP Top 10 -julkaisussa (https://owasp.org/www-project-top-ten/) kuvatut tietoturvaongelmat. Lisätietoa löytyy kunkin otsikon takaa löytyvästä linkistä. Vastaavat otsikot löytyvät myös OWASP Top 10 -julkaisun etusivulta.

Tämä kuvaus on liitetty Webropol tietoturvakuvauksen liitteeksi.

Liitteet 2 ja 3, ISO/IEC 27001:2022 sertifikaatti

Sisällys

1 A01:2021-Broken Access Control 1
2 A02:2021-Cryptographic Failures 1
3 A03:2021-Injection 1
4 A04:2021-Insecure Design 2
5 A05:2021-Security Misconfiguration 2
6 A06:2021-Vulnerable and Outdated Components 2
7 A07:2021-Identification and Authentication Failures 2
8 A08:2021-Software and Data Integrity Failures 3
9 A09:2021-Security Logging and Monitoring Failures 3
10 A10:2021-Server-Side Request Forgery 3

1 A01:2021-Broken Access Control

Pääsynhallinta toteutettu Microsoftin .NET frameworkin parhaiden käytäntöjen mukaan. Sovelluksesta lähtee hälytyksiä järjestelmänvalvojille toistuvista virheistä ja haitallisista toiminnoista. Sovelluspalvelimen juuressa ei ole tietoa liittyen git, varmuuskopioihin tai muuhun metadataan. Käyttäjähallinnassa voidaan määrittää käyttäjien pääsy vain tiettyihin resursseihin. Muutoksia voidaan seurata päivämäärä-, kellonaika- ja käyttäjätasolla, jolloin toimintojen jäljittäminen on mahdollista.

Lisätietoa: https://learn.microsoft.com/en-us/aspnet/mvc/overview/security/

2 A02:2021-Cryptographic Failures

Sovellus ei käytä TLS 1.2 vanhempia protokollia ja heikoksi tunnettuja salausmenetelmiä. Sovellus ei ole haavoittuvainen tunnetuille haavoittuvuuksille, kuten: Heartbleed, CCS, Ticketbleed, ROBOT, Secure Renegotiation, Secure-Client-Initiated Renegotiation, CRIME, BREACH, POODLE, TLS_FALLBACK_SCSV, SWEET32, FREAK, DROWN, LOGJAM, BEAST, LUCKY13, Winshock tai RC4.

Webropol käyttää avainten välityksessä Forward Secrecyä (FS). Sovellus tarjoaa seuraavia salausmenetelmiä:

TLSv1.2	0xc030	ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.2	0xc02f	ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.2	0x009f	DHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.2	0x009e	DHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.3	0x1302	TLS_AES_256_GCM_SHA384
TLSv1.3	0x1303	TLS_CHACHA20_POLY1305_SHA256
TLSv1.3	0x1301	TLS_AES_128_GCM_SHA256
TLSv1.3	0x1304	TLS_AES_128_CCM_SHA256

Sovelluksen käyttämät elliptiset käyrät ovat *prime256v1, secp384r1, secp521r1, X25519 ja X448*, käytössä oleva Diffie Hellman ryhmä on Group 14 (2048-bit) RSA avaimen pituus on 2048 bittiä. Tietokanta on salattu Microsoftin omalla salauksella, joka on Transparent data encryption (TDE). Tietokannan ja sovelluspalvelimen välinen liikenne on salattu.

Lisätietoa: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16

3 A03:2021-Injection

Käytössä on .NET frameworkin oma input validointikirjasto https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-input-validation

Lisäksi kaikki käyttäjien syötteet ja käyttäjälle palautuva tieto sanitoidaan (sisällön tarkastus). SQL-kyselyissä hyödynnetään valmisteltuja SQL-käskyjä ja kyselyt ovat parametrisoituja.

Lisätietoa: https://en.wikipedia.org/wiki/Prepared_statement

4 A04:2021-Insecure Design

Webropol on suunniteltu Microsoftin .net framework parhaiden käytäntöjen mukaan. Järjestelmä on testattu F-Securen toimesta 2021. Kehitys-, QA- ja tuotantoympäristöt on määritetty samalla tavalla ja tietoturvatestaamista tehdään QA-ympäristössä, jolloin haavoittuvuudet voidaan replikoida ja korjata muissa ympäristöissä. Sovelluksen arkkitehtuuri on segmentoitu käyttäen palomuureja ja kuormantasaajaa. Sovelluksessa on käytössä tietoturvaotsakkeet (security-headers).

Lisätietoa: https://securityheaders.com/?q=https%3A%2F%2Fnew.webropolsurveys.com

Lisätietoa: https://learn.microsoft.com/en-us/aspnet/mvc/

5 A05:2021-Security Misconfiguration

Verkkoliikenne on sallittu vain porttiin 443. Koko ympäristö on kovennettu vuonna 2021 F-securen auditoinnin yhteydessä. Kovennukset tarkistetaan seuraavassa tietoturva-auditoinnissa. Sovellusta testataan kuukausittain mahdollisilta konfiguraatiovirheiltä tai muutoksilta. Sovelluksessa on käytössä tietoturvaotsakkeet (security-headers).

Lisätietoa: https://securityheaders.com/?q=https%3A%2F%2Fnew.webropolsurveys.com

6 A06:2021-Vulnerable and Outdated Components

Palvelinalustan komponentit skannataan ylläpitäjän (3-osapuoli) toimesta. Ylläpitäjä ilmoittaa palvelinalustaan kohdistuvista haavoittuvuuksista ja päivittää alustakomponentit. Sovelluksen komponentit skannataan 4 kertaa vuodessa, komponentit, joissa havaitaan haavoittuvuuksia, päivitetään heti kun mahdollista.

7 A07:2021-Identification and Authentication Failures

Sovellus lukitsee käyttäjätunnukset viiden (5) väärinkirjautumisen jälkeen. Lukitus voidaan poistaa organisaation pääkäyttäjän toimesta. Sovellukseen voidaan myös ottaa 2-vaiheinen tunnistautuminen käyttöön, salasanapolitiikkaa voidaan määrittää asiakasorganisaation haluamalle tasolle.

API-kutsuissa on käytössä myös ”Bearer token”, jolla palvelimelta kysytään resursseja.
https://blog.restcase.com/4-most-used-rest-api-authentication-methods/ .

Sovellukseen voidaan myös kirjautua käyttäen SSO:ta HAKA federoinnilla, jolloin pääsynhallinta on organisaation käsissä.

8 A08:2021-Software and Data Integrity Failures

Sovelluskehityksessä on otettu huomioon OWASP-suositukset. Kirjastojen säilytyspaikat ovat ensisijaisesti luotettuja. Webropol käyttää NuGet (https://www.nuget.org/) .NET kirjastojen asentamiseen. CI/CD puoli on konfiguroitu parhaiden käytänteiden mukaan. Ohjelmistokoodi tarkistetaan staattisesti useamman henkilön toimesta, millä varmistetaan koodin laadun ylläpitäminen. http://www.rharbridge.com/wp-content/uploads/2010/08/Code-Review-Checklist.docx, https://medium.com/c-sharp-progarmming/c-best-practices-and-code-review-checklist-25880d9606, https://security-code-scan.github.io/

Ohjelmistokoodia säilytetään omassa versionhallintajärjestelmässä ja koodistoon on järjestetty pääsynhallinta, mistä Webropol vastaa. Versionhallinnasta voidaan seurata koodistoon tehtyjä muutoksia. Kehitysympäristöt on erotettu tuotantoympäristöstä. Kehitysympäristössä, integraatio- ja hyväksymistestaus on eriytetty.

9 A09:2021-Security Logging and Monitoring Failures

Sovelluksesta lokitetaan kaikki http-kutsut. Sovelluksessa on käytössä audit ja virhelokitus. Palvelinalustassa kerätään myös audit ja IIS -lokit. Virheistä ja haitalliseksi havaituista toiminnoista muodostuu hälytyksiä, johon voidaan reagoida.

10 A10:2021-Server-Side Request Forgery

Sovelluksessa sanitoidaan kaikki käyttäjän kirjaamat syötteet. Sovelluksesta on poistettu käytöstä http-uudelleenohjaukset ja verkkoliikenne on sallittu porttiin 443 (https). Käyttämättömät URL schemat poistetaan käytöstä. Sisäisten palveluiden pääsyrajoitukset on määritetty asianmukaisesti

Sertifikaatti
No. 9743-09

Certificate

Kiwa Sertifiointi Oy on myöntänyt tämän sertifikaatin, joka varmentaa, että organisaation

Telia Finland Oyj
Helsinki

tietoturvallisuuden hallintajärjestelmä täyttää seuraavan standardin vaatimukset

ISO/IEC 27001:2022

Sertifiointiin sisältyvä toiminta

Tietoturvan hallintajärjestelmän soveltamisala kattaa Telia Finland Oyj:n toiminnot, joilla hallitaan ja tuotetaan sähköisiä viestintäpalveluita, IT- ja laitepalveluita ja luottamuspalveluita sekä näihin liitännäisiä palveluita yritysasiakkaille. Soveltamisalan ulkopuolelle jäävät operaattoreiden tukkuliiketoiminta sekä Helsinki Datacenterin palvelut.
Sertifioidut toimipaikat liitteessä.
Soveltuvuuslausunto versio 2.0 (2025-11-11)

Sertifikaatti on myönnetty 2025-12-03
(alkuperäinen myönnetty 2017-12-14).
Sertifikaatti on voimassa 2026-12-14.

Maija Vanttaja, toimitusjohtaja

Sertifikaatti on voimassa edellyttäen, että organisaation tietoturvallisuuden hallintajärjestelmä täyttää edellä mainitun standardin ja yleisen ohjeen ABC 200 vaatimukset. Sertifikaatin voimassaolon voi tarkistaa osoitteesta www.kiwa.com/fi.

kiwa CERTIFIED ISO/IEC 27001 Kiwa Sertifiointi Oy

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

FINAS Finnish Accreditation Service S002 (EN ISO/IEC 17021-1)

KPMG
IT Certification Ltd

Certificate of Registration

KPMG IT Certification Ltd certifies that the following organization

Webropol Oy

complies with the requirements of standard

ISO/IEC 27001:2022

for the following scope of registration

Information Security Management System (ISMS) covering Webropol's information processing environments and systems, personnel and supporting services used to develop, operate and maintain Webropol SaaS service, including application development, hosting and cloud-based IT infrastructure in Finland. Office in Helsinki, Finland
Statement of Applicability version 1.0 (30.10.2025)

Certification number
FI251222-223

Olli Knuuti, COO
KPMG IT Certification Ltd

Issue Date	Original Issuing Date	Expiration Date
December 22nd, 2025	December 22nd, 2025	December 22nd, 2028

FINAS
Finnish Accreditation Service
S045 (EN ISO/IEC 17021-1)

To verify that this certificate is current, please refer to the KPMG IT Certification Ltd:
sertifiointi@kpmg.fi

KPMG IT Certification Ltd | T: +358 20 760 3000
P.O. Box 1037, Töölönlahdenkatu 3 A | FI-00101 Helsinki, Finland