					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P03S					Asiakirjan nimi: **Hyväksyttävän käytön politiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Oikeudellinen huomautus (tekijänoikeudet ja käyttörajoitukset)

(C) 2025 Clarysec LLC. All rights reserved.

Tämä asiakirja on Clarysec LLC:n immateriaalioikeudellista omaisuutta. Tämän asiakirjan mitään osaa ei saa kopioida, käyttää uudelleen, jakaa tai muokata kaupallisiin tai käyttöönottoon liittyviin tarkoituksiin ilman nimenomaista kirjallista lupaa.

Luvaton käyttö on ehdottomasti kielletty ja voi johtaa oikeudellisiin toimiin.

Lisensointia koskevissa asioissa ota yhteyttä: info@clarysec.com

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Kohta 5	Olennainen politiikan yleisen soveltamisalan ja toimeenpanon kannalta
ISO/IEC 27002:2022	5.10, 5.11, 5	Ohjeistaa hyväksyttävän käytön vaatimuksia ja kontrolleja
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Kattaa järjestelmien ja laitteiden käytön, valvonnan ja käyttäjien koulutuksen
EU:n GDPR	Artiklat 5(1)(f), 32	Tietojen eheys ja luottamuksellisuus sekä tietoturvatoimenpiteet
EU:n NIS2-direktiivi	Artikla 21(2)(b)	Edellyttää asianmukaisia tietoturva- ja hyväksyttävän käytön politiikkoja
EU:n DORA-asetus	Artikla 9	TVT-riskienhallintapolitiikka, kontrollit ja toimeenpano
COBIT 2019	DSS05, BAI08	Tietoturvapalvelut ja tiedonhallinta

1. Tarkoitus

1.1. Tämä politiikka määrittää organisaation tarjoamien järjestelmien, laitteiden, internetyhteyden, sähköpostin, pilvipalveluiden sekä liiketoiminnassa käytettävien henkilökohtaisten laitteiden hyväksyttävän, vastuullisen ja turvallisen käytön.

1.2. Tämän politiikan tarkoituksena on varmistaa, että henkilöt ymmärtävät velvollisuutensa käyttäessään organisaation IT-resursseja sekä suojatessaan tietojen eheyttä, yksityisyyttä ja toiminnan jatkuvuutta.

1.3. Tämä politiikka tukee ISO/IEC 27001:2022 -standardin vaatimustenmukaisuutta määrittämällä käyttäjille selkeät toimintasäännöt oikeudellisten, sopimuksellisten ja sääntelyvaatimusten mukaisesti.

2. Soveltamisala

2.1. Tätä politiikkaa sovelletaan kaikkiin henkilöihin, jotka käyttävät, hallinnoivat tai muutoin käsittelevät organisaation järjestelmiä tai tietoja, mukaan lukien:

2.1.1. työntekijät ja sopimuskumppanit

2.1.2. määräaikaiset työntekijät ja harjoittelijat

2.1.3. ulkoiset IT-palveluntarjoajat

2.2. Politiikka kattaa:

2.2.1. organisaation omistamat tietokoneet, puhelimet ja tabletit

2.2.2. liiketoimintakäyttöön hyväksytyt henkilökohtaiset laitteet (BYOD)

2.2.3. organisaation verkot, pilvialustat ja ohjelmistopalvelut

2.2.4. internetyhteydet, sähköpostijärjestelmät, jaetun tallennustilan ja liiketoimintasovellukset

2.3. Tätä politiikkaa sovelletaan kaikissa työympäristöissä — toimipaikalla, etätyössä ja hybridityössä — kaikkina työaikoina.

3. Tavoitteet

3.1. Määrittää, mitä pidetään IT-järjestelmien hyväksyttävänä ja ei-hyväksyttävänä käyttönä.

3.1.1. Vähentää väärinkäytöstä, luvattomasta käytöstä tai haittaohjelmien käyttöönotosta aiheutuvia tietoturvariskejä.

3.1.2. Suojata liiketoimintatietoja, asiakastietoja ja organisaation mainetta.

3.1.3. Asettaa sitovat säännöt ja varmistaa vastuiden jäljitettävyys kaikille käyttäjille.

3.1.4. Tukea seurantaa ja vaatimustenmukaisuuden valvontaa rikkomusten havaitsemiseksi varhaisessa vaiheessa ja korjaavien toimenpiteiden toteuttamiseksi.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. Hyväksyy tämän politiikan ja varmistaa, että sen soveltamiseen on käytettävissä riittävät resurssit ja toimivaltuudet.

4.1.2. Tarkastaa ja hyväksyy kaikki tätä politiikkaa koskevat poikkeukset.

4.2. IT-päällikkö tai ulkoinen IT-palveluntarjoaja

4.2.1. Ylläpitää luetteloita hyväksytystä ohjelmisto- ja laitekannasta.

4.2.2. Määrittää laitteet siten, että hyväksyttävän käytön säännöt toteutuvat käytännössä (esimerkiksi sisältösuodatus ja käytön lokitus).

4.2.3. Seuraa käyttöä mahdollisten rikkomusten havaitsemiseksi ja tutkii tapahtumat.

4.2.4. Varmistaa, että liiketoimintakäytössä käytettävät henkilökohtaiset laitteet (BYOD) on hyväksytty ja suojattu asianmukaisesti.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1. Vuosittainen katselmointi

9.1.1. IT-päällikön on katselmoitava tämä politiikka vuosittain, ja toimitusjohtajan on annettava lopullinen hyväksyntä sen ajantasaisuuden varmistamiseksi suhteessa teknologian käyttötapoihin, kehittyviin riskeihin ja vaatimustenmukaisuusvelvoitteisiin.

9.2. Katselmoinnin välitarkistusta edellyttävät tilanteet

9.2.1. Katselmointi on tehtävä myös seuraavissa tilanteissa:

9.2.2. uudet järjestelmät tai teknologiat (esimerkiksi uusi pilvipalvelu tai päätelaitealusta)

9.2.3. merkittävät politiikkarikkomukset

9.2.4. päivitetty lainsäädäntö tai sopimusehdot, jotka vaikuttavat IT-resurssien käyttöön

9.3. Muutosten dokumentointi

9.3.1. Kaikki päivitykset on kirjattava versiolokiin, joka sisältää:

9.3.1.1. versionumeron

9.3.1.2. katselmointipäivän

9.3.1.3. yhteenvedon muutoksista

9.3.1.4. hyväksyvän tahon

9.4. Politiikan viestintä

9.4.1. Tämän politiikan päivitetyt versiot on toimitettava kaikille käyttäjille, joita muutos koskee. Työntekijöiden on osana tietoturvatietoisuusvelvoitteitaan vahvistettava vastaanottaneensa politiikan ja ymmärtäneensä sen.

10. Liittyvät politiikat ja yhteydet

10.1. Tämä politiikka muodostaa yhdessä muiden pk-yrityksille tarkoitettujen politiikkojen kanssa kokonaisuuden, jolla varmistetaan tietoturvavastuiden kattava hallinta:

10.1.1. P4S – Käyttövalvontapolitiikka: Määrittää sallitun käytön ja käyttöoikeusrajoitusten tekniset ja menettelylliset kontrollit.

10.1.2. P8S – Tietoturvatietoisuuden ja koulutuksen politiikka: Määrittää käyttäjien koulutuksen hyväksyttävän käytön rajoista ja ilmoitusvelvollisuuksista.

10.1.3. P9S – Etätyöpolitiikka: Säätelee organisaation järjestelmien käyttöä toimipaikan ulkopuolella ja kotiympäristössä.

10.1.4. P17S – Tietosuojan ja yksityisyyden politiikka: Määrittää henkilötietojen käsittelyä koskevat säännöt, jotka liittyvät hyväksyttävän käytön seurantaan ja BYOD-käyttöön.

10.1.5. P30S – Tietoturvapoikkeamien hallintapolitiikka: Määrittää menettelyt hyväksyttävän käytön ehtojen rikkomusten ja väärinkäytösten tutkimiseksi ja käsittelemiseksi.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 5.10 – Edellyttää organisaatioita määrittämään ja soveltamaan tietovarojen hyväksyttävää käyttöä.

11.2. ISO/IEC 27002

11.2.1. Kontrolli 5.10 – Antaa ohjeet järjestelmien hyväksyttävästä käytöstä, mukaan lukien sallitut ja kielletyt toimintatavat.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Käsittelee järjestelmien käytön hallintaa, mukaan lukien henkilökohtaiset laitteet.

11.3.2. AC-20 – Edellyttää ulkoisten järjestelmien hyväksyntää ja seurantaa.

11.3.3. AT-2 – Korostaa käyttäjien kouluttamista hyväksyttävän käytön käytännöistä.

11.4. EU:n GDPR

11.4.1. Artikla 5(1)(f) – Edellyttää henkilötietojen eheyttä ja luottamuksellisuutta, jotka voivat vaarantua käyttäjän väärinkäytön seurauksena.

11.4.2. Artikla 32 – Edellyttää teknisten ja organisatoristen toimenpiteiden toteuttamista järjestelmien ja tietojen suojaamiseksi.

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(b) – Edellyttää asianmukaisia tietoturvapolitiikkoja, mukaan lukien hyväksyttävää käyttöä koskevat säännöt, kyberuhkien lieventämiseksi.

11.6. EU:n DORA-asetus

11.6.1. Artikla 9 – Edellyttää TVT-riskienhallintapolitiikkoja, joihin sisältyvät käytön kontrollit ja toimeenpanomekanismit.

11.7. COBIT 2019

11.7.1. DSS05 – Tietoturvapalvelujen hallinta: korostaa politiikkaperusteista käyttäjätoiminnan hallintaa.

11.7.2. BAI08 – Tiedon hallinta: käsittelee tietoisuutta politiikan mukaisista vastuista ja hyväksyttävän käytön koulutusta.