

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P03S				Titlu tad-dokument: Politika dwar l-Użu Aċċettabbli							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025		Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	Data tar-reviżjoni	Bidliet	Ivvedut minn	Sid tal-proċess

Approvazzjonijiet			
Isem	Pożizzjoni	Data	Firma

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)

(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettuali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 5	Rilevanti għall-kamp ta' applikazzjoni u għall-implimentazzjoni ġenerali tal-politika
ISO/IEC 27002:2022	5.10, 5.11, 5	Tipprovdi gwida dwar ir-rekwiżiti u l-kontrolli għall-użu aċċettabbli
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Ikopri l-użu tas-sistemi u tal-apparat, il-monitoraġġ u t-taħriġ tal-utenti
GDPR tal-UE	Artikoli 5(1)(f), 32	Integrità u kunfidenzjalità tad-data u miżuri ta' sigurtà
Direttiva NIS2 tal-UE	Artikolu 21(2)(b)	Tirrikjedi politiki xierqa ta' sigurtà u ta' użu aċċettabbli
DORA tal-UE	Artikolu 9	Politika ta' ġestjoni tar-riskju tal-ICT, kontrolli u implimentazzjoni
COBIT 2019	DSS05, BAI08	Servizzi ta' sigurtà u ġestjoni tal-għarfien

1. Għan

1.1. Din il-politika tiddefinixxi l-użu aċċettabbli, responsabbli u sigur tas-sistemi, l-apparat, l-aċċess għall-internet, l-email, is-servizzi cloud u kwalunkwe apparat personali użat għal skopijiet tan-negożju li jingħataw jew jiġu awtorizzati mill-kumpanija.

1.2. Din tiżgura li l-individwi jifhmu l-obbligi tagħhom meta jużaw ir-riżorsi tal-IT tal-organizzazzjoni, u tipproteġi l-integrità tad-data, il-privatezza u l-kontinwità operattiva.

1.3. Din il-politika tappoġġa l-konformità ma' ISO/IEC 27001:2022 billi tistabilixxi standards ċari ta' mgħiba għall-utenti, allinjati mar-rekwiżiti legali, kuntrattwali u regulatorji.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għall-individwi kollha li jaċċessaw, jimmaniġġjaw jew jinteraġixxu mas-sistemi jew mad-data tal-kumpanija, inklużi:

- 2.1.1. Impjegati u kuntratturi
- 2.1.2. Haddiema temporanji jew interns
- 2.1.3. Fornituri esterni ta' servizzi tal-IT

2.2. Din tkopri:

- 2.2.1. Kompjuters, telefowns u tablets tal-kumpanija
- 2.2.2. Apparati personali approvati għall-użu fin-negożju (BYOD)
- 2.2.3. Networks tal-kumpanija, pjattaformi cloud u servizzi ta' software
- 2.2.4. Aċċess għall-internet, sistemi tal-email, hażna kondiviża u applikazzjonijiet tan-negożju

2.3. Din il-politika tapplika fl-ambjenti kollha tax-xogħol — fuq il-post, b'mod remot jew b'mod ibridu — u matul il-ħinijiet kollha tan-negożju.

3. Obiettivi

3.1. Jiddefinixxu x'jikkostitwixxi użu aċċettabbli u użu mhux aċċettabbli tas-sistemi tal-IT.

3.1.1. Inaqqsu r-riskji ta' sigurtà kkawżati minn użu ħażin, aċċess mhux awtorizzat jew introduzzjoni ta' malware.

3.1.2. Jipproteġu d-data tan-negozju, l-informazzjoni tal-klijenti u r-reputazzjoni tal-kumpanija.

3.1.3. Jistabbilixxu regoli infurzabbli u jiżguraw ir-responsabbiltà tal-utenti kollha.

3.1.4. Jappoġġaw il-monitoraġġ u l-konformità biex il-ksur jiġi identifikat minn kmieni u tittiehed azzjoni korrettiva.

4. Rwoġi u responsabbiltajiet

4.1. Maniġer Ġenerali

4.1.1. Japprova din il-politika u huwa responsabbli biex jiżgura li jkunu disponibbli r-riżorsi u l-awtorità meħtieġa għall-implimentazzjoni tagħha.

4.1.2. Jagħmel ir-rieżami u jawtorizza kwalunkwe eċċezzjoni għal din il-politika.

4.2. Maniġer tal-IT jew Fornitur Estern tal-IT

4.2.1. Iżomm inventarji tas-software u tal-hardware approvati.

4.2.2. Jikkonfigura l-apparat biex jiġu infurzati r-regoli tal-użu aċċettabbli, pereżempju permezz ta' filtrazzjoni tal-kontenut u logging tal-aċċess.

4.2.3. Jimmonitorja l-użu għal ksur potenzjali u jinvestiga l-inċidenti.

4.2.4. Jiżgura li apparati personali (BYOD) ikunu awtorizzati u siguri jekk jintużaw għal skopijiet tan-negozju.

[... Is-sezzjonijiet 4.3–8 mhumiex inkluzi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiziti għar-rieżami u l-aġġornament

9.1. Rieżami annwali

9.1.1. Din il-politika għandha tiġi rieżaminata kull sena mill-Maniġer tal-IT, bl-approvazzjoni finali tal-Maniġer Ġenerali, biex jiġi żgurat li tibqa' allinjata max-xejriet tal-użu tat-teknoloġija, mar-riskji emergenti u mal-obbligi ta' konformità.

9.2. Kawżi għal rieżami interim

9.2.1. Ir-rieżamijiet għandhom isiru wkoll b'reazzjoni għal:

9.2.2. Sistemi jew teknoloġiji ġodda (eż. servizz cloud ġdid jew pjattaforma ġdida tal-endpoints)

9.2.3. Ksur sinifikanti tal-politika

9.2.4. Liġijiet aġġornati jew termini kuntrattwali li jaffettwaw l-użu tal-IT

9.3. Dokumentazzjoni tal-bidliet

9.3.1. L-aġġornamenti kollha għandhom jiġu rreġistrati f'log tal-verżjonijiet li jinkludi:

9.3.1.1. Numru tal-verżjoni

9.3.1.2. Data tar-rieżami

9.3.1.3. Sommarju tal-bidliet

9.3.1.4. Awtorità li approvat

9.4. Komunikazzjoni tal-politika

9.4.1. Verżjonijiet riveduti ta' din il-politika għandhom jiġu kondiviżi mal-utenti kollha affettwati. L-impjegati għandhom jikkonfermaw li rċevewha u fehmuha bħala parti mill-obbligi tagħhom ta' għarfien dwar is-sigurtà.

10. Politiki relatati u rabtiet

10.1. Din il-politika għandha tinqara flimkien ma' diversi politiki oħra tal-SME biex tiżgura kopertura komprensiva tar-responsabbiltajiet tas-sigurtà:

10.1.1. P4S – Politika dwar il-Kontroll tal-Aċċess: Tiddefinixxi l-implimentazzjoni teknika u proċedurali tal-użu permess u tar-restrizzjonijiet fuq il-kontijiet.

10.1.2. P8S – Politika dwar l-Għarfien dwar is-Sigurtà tal-Infurmazzjoni u t-Taħriġ: Tipprovdi edukazzjoni lill-utenti dwar il-limiti tal-użu aċċettabbli u l-obbligi ta' rapportar.

10.1.3. P9S – Politika dwar ix-Xogħol Remot: Tirregola l-użu tas-sistemi tal-kumpanija f'ambjenti barra l-post tax-xogħol jew fid-dar.

10.1.4. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tapplika r-regoli tal-immaniġġjar tad-data personali li jinteraġixxu mal-monitoraġġ tal-użu aċċettabbli u mal-BYOD.

10.1.5. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tirregola l-proċeduri għall-investigazzjoni u r-rispons għal użu ħażin jew ksur tat-termini tal-użu aċċettabbli.

11. Standards u oqfsa ta' referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 5.10 – Tirrikjedi li l-organizzazzjonijiet jiddefinixxu u japplikaw użu aċċettabbli tal-assi tal-infurmazzjoni.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.10 – Jipprovdi linji gwida għall-użu aċċettabbli tas-sistemi, inklużi mgħibiet permessi u pprojbiti.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Jindirizza l-kontroll tal-użu tas-sistema, inklużi apparati personali.

11.3.2. AC-20 – Jirrikjedi awtorizzazzjoni u monitoraġġ ta' sistemi esterni.

11.3.3. AT-2 – Jenfasizza t-taħriġ tal-utenti dwar Prattiki ta' użu aċċettabbli.

11.4. GDPR tal-UE

11.4.1. Artikolu 5(1)(f) – Jirrikjedi l-integrità u l-kunfidenzjalità tad-data personali, li jistgħu jiġu kompromessi b'użu ħażin mill-utent.

11.4.2. Artikolu 32 – Jirrikjedi l-implimentazzjoni ta' miżuri tekniċi u organizzattivi biex jiġu protetti s-sistemi u d-data.

11.5. Direttiva NIS2 tal-UE

11.5.1. Artikolu 21(2)(b) – Jirrikjedi politiki xierqa ta' sigurtà, inklużi regoli dwar l-użu aċċettabbli, biex jitnaqqas it-theddid ċibernetiku.

11.6. DORA tal-UE

11.6.1. Artikolu 9 – Jirrikjedi politiki ta' ġestjoni tar-riskju tal-ICT, li jinkludu kontrolli tal-użu u mekkaniżmi ta' infurzar.

11.7. COBIT 2019

11.7.1. DSS05 – Immaniġġjar tas-Servizzi ta' Sigurtà: Jenfasizza kontroll ibbażat fuq il-politika fuq l-imġiba tal-utent.

11.7.2. BAI08 – Immaniġġjar tal-Għarfien: Jindirizza l-għarfien tar-responsabbiltajiet tal-politika u l-edukazzjoni dwar l-użu aċċettabbli.