acceptable_use_policy

Erabilera Onargarriaren Politika (AUP)

Zabala Gailetak S.A

Dokumentuaren IDa: AUP-001
Bertsioa: 1.0
Data: 2026ko Urtarrilaren 8a
Sailkapena: Barne Erabilera
Jabea: Informazioaren Segurtasuneko Arduradun Nagusia (CISO)
Berrikuspen Maiztasuna: Urterokoa
Hurrengo Berrikuspen Data: 2027ko Urtarrilaren 8a

---

1. Dokumentuaren Kontrola

1.1 Bertsio Historia

Bertsioa	Data	Egilea	Aldaketak
1.0	2026-01-08	CISO	Hasierako politikaren sorrera

1.2 Onarpena

Rola	Izena	Sinadura	Data
Zuzendari Nagusia (CEO)	[Izena]		
Informazioaren Segurtasuneko Arduradun Nagusia (CISO)	[Izena]		
Giza Baliabideetako Kudeatzailea	[Izena]		
Aholkulari Juridikoa	[Izena]		

---

2. Helburua eta Esparrua

2.1 Helburua

Erabilera Onargarriaren Politika (AUP) honek Zabala Gailetak-en informazio-teknologia baliabideen erabilera onargarria eta onartezina definitzen du. Helburua da:

- Erakundea segurtasun arriskuetatik babestea
- Lege eta arau baldintzak betetzen direla ziurtatzea
- Produktibitatea eta lan-giro profesionala mantentzea
- Enpresaren ospea eta aktiboak babestea

- Langileen eskubideak eta erantzukizunak argitzea

2.2 Esparrua

Politika hau honako hauei aplikatzen zaie:

- **Erabiltzaile Guztiak:** Langileak (finkoak, aldi baterakoak, kontratatuak), aholkulariak, kontratistak, bisitariak eta hirugarrenak
- **Gailu Guztiak:** Enpresaren jabetzakoak eta gailu pertsonalak (BYOD) negozio helburuetarako erabiltzen direnean
- **Baliabide Guztiak:** IT sistemak, sareak, posta elektronikoa, interneta, softwarea, gailu mugikorrak, hodeiko zerbitzuak eta datuak
- **Kokapen Guztiak:** Bulegoa, produkzio instalazioa, etxea, urruneko lana, bezeroen guneak, bidaiak

2.3 Betetzea

Politika hau betetzea derrigorrezkoa da. Urraketek honakoak ekar ditzakete:

- Diziplina ekintzak (ahozko ohartarazpena, idatzizko ohartarazpena, etenaldia, kaleratzea)
- Sarbide pribilegioak baliogabetzea
- Lege ekintzak (jazarpen kriminala edo zibila)
- Kalteengatiko erantzukizun finantzarioa

Langileek urtero aitortu behar dute politika hau ulertzen dutela.

---

3. Printzipio Orokorrak

3.1 Negozio Helburua

IT baliabideak negozio helburuetarako eskaintzen dira. Erabilera pertsonal mugatua onartzen da, baldin eta:

- Ez badu lan eginkizunetan oztoporik sortzen
- Ez badu baliabide esanguratsurik kontsumitzen
- Ez badu politika xedapenik urratzen
- Lege eta araudi guztiak betetzen baditu

Zabala Gailetak-ek eskubidea du enpresaren sistemetako edukia monitorizatzeko, sartzeko eta ezagutarazteko politika betetzen dela ziurtatzeko, jokabide okerrak ikertzeko edo legezko betebeharrak betetzeko.

3.2 Jokabide Profesionala

Erabiltzaileek:

- Profesionalki eta etikoki jokatu behar dute
- Jabetza intelektualaren eskubideak errespetatu behar dituzte
- Informazio konfidentziala babestu behar dute
- Interes gatazkak saihestu behar dituzte
- Segurtasun intzidenteak eta politika urraketak jakinarazi behar dituzte

3.3 Pribatutasun Itxaropenik Ez

Erabiltzaileek ez dute pribatutasun itxaropenik izan behar enpresaren IT baliabideak erabiltzean. Zabala Gailetak-ek eskubidea du:

- Sare trafikoa eta sistema erabilera monitorizatzeko
- Posta elektronikoa, fitxategiak eta interneteko jarduera berrikusteko
- Sarbide eta autentifikazio gertaerak erregistratzeko
- Gailuak ikuskatzeko (enpresaren jabetzakoak edo enpresaren datuak dituzten BYOD)

Monitorizazioa Espainiako lan legearen eta langileen pribatutasun eskubideen arabera egiten da. Argi eta garbi pertsonal gisa markatutako komunikazioak errespetatuko dira legez beharrezkoa den lekuetan.

---

4. Kontu eta Autentifikazio Kudeaketa

4.1 Erabiltzaile Kontuak

Kontu Jaulkipena:

- Erabiltzaile kontuak IT-k jaulkitzen ditu erabiltzailearen kudeatzailearen baimenarekin
- Erabiltzaile bakoitzak erabiltzaile-izen bakarra jasotzen du (ez dago partekatutako konturik)
- Kontuak pertsonalak eta besterenezinak dira

Kontu Erantzukizunak:

- Erabiltzaileak beren kontuaren azpian egindako jarduera guztien erantzule dira
- Erabiltzaileek ez dituzte beren kredentzialak inorekin partekatu behar
- Erabiltzaileek saioa itxi behar dute lan-estazioa zaintzarik gabe uztean
- Erabiltzaileek galdutako, lapurtutako edo arriskuan jarritako kredentzialak berehala jakinarazi behar dituzte

Kontu Bizi-zikloa:

- Kontuak kontratazio/onboarding-etik 24 orduko epean sortzen dira
- Kontuak berehala desgaitzen dira amaiera edo baimen luzearen kasuan
- Kontu inaktiboak (>90 egun) automatikoki desgaitzen dira
- Desgaitutako kontuak 30 egunen buruan ezabatzen dira (datuak atxikipen politikaren arabera artxibatzen dira)

4.2 Pasahitz Baldintzak

Ikus Pasahitz Politika dedikatua (PWD-001) baldintza zehatzetarako. Laburpena:

- **Gutxieneko luzera:** 12 karaktere (14 kontu pribilegiatuetarako)
- **Konplexutasuna:** Maiuskula, minuskula, zenbakia, karaktere berezia
- **Iraungitzea:** 90 egun (180 egun MFA gaituta badago)
- **Historia:** Ezin dira azken 12 pasahitzak berrerabili
- **Debekatuta:** Hiztegi hitzak, informazio pertsonala, enpresa izena, eredu arruntak

Pasahitz Kudeaketa:

- Ez idatzi inoiz pasahitzak (erabili onartutako pasahitz kudeatzailea)
- Ez partekatu inoiz pasahitzak (IT langileekin edo kudeatzaileekin barne)
- Ez erabili pasahitz bera sistema anitzetarako

- Aldatu pasahitza berehala arriskua susmatzen bada

4.3 Faktore Anitzeko Autentifikazioa (MFA)

MFA **derrigorrezkoa** da honakoetarako:

- Urruneko sarbidea (VPN)
- Administratzaile/pribilegiatutako kontuak
- Bezeroen datuetara edo finantza sistemetara sarbidea
- Hodeiko zerbitzuak (M365, AWS, GitHub)

MFA **gomendagarria** da honakoetarako:

- Erabiltzaile kontu estandarrak (bulegoko lan-estazioak)

Onartutako MFA Metodoak:

1. Autentifikatzaile aplikazioa (Microsoft Authenticator, Google Authenticator, Authy)
2. Hardware tokena (YubiKey administratzaileentzat)
3. SMS (gutxien hobetsia, besteak ez badaude eskuragarri soilik)

Debekatuta: Email bidezko MFA (autentifikazio nagusiaren kanal berean)

---

5. Ordenagailu eta Lan-estazio Erabilera

5.1 Segurtasun Fisikoa

Lan-estazio Segurtasuna:

- Blokeatu pantaila mahaia uztean (Windows+L edo Ctrl+Alt+Delete → Lock)
- Pantaila blokeo automatikoa 5 minutu inaktibitate ondoren
- Ez utzi baimenik gabeko pertsonei zure lan-estazioa erabiltzen
- Berehala jakinarazi galdutako edo lapurtutako ekipamendua

Mahai Garbia Politika:

- Ziurtatu edo txikitu dokumentu konfidentzialak erabiltzen ez direnean
- Ez utzi informazio sentikorra ikusgai mahaian
- Blokeatu informazio sentikorra duten bulegoak eta armairuak
- Ez idatzi pasahitzak

Pantaila Garbia Politika:

- Kokatu pantailak ikuspegi publikotik urrun ahal den neurrian
- Erabili pribatutasun iragazkiak espazio publikoetan lan mugikorra egitean
- Itxi aplikazio sentikorrak erabiltzen ez direnean

5.2 Software Instalazioa

Onartutako Softwarea:

- IT-k onartutako softwarea bakarrik instalatu daiteke enpresaren gailuetan
- Eskatu softwarea IT helpdesk-aren bidez (software eskaera inprimakia)

- IT-k onartutako aplikazioen zerrenda zuria mantentzen du

Debekatutako Softwarea:

- Baimenik gabeko softwarea, doako softwarea edo sharewarea
- Pirata edo lizentziarik gabeko softwarea
- Peer-to-peer fitxategi partekatzea (BitTorrent, etab.)
- VPN edo proxy zerbitzu pertsonalak (sare korporatiboa saihestuz)
- Kriptomoneta meatzaritza softwarea
- Hacking tresnak (segurtasun talderako espresuki baimenduta ez badaude)
- Iturri ez-fidagarrietako softwarea

Nabigatzaile Luzapenak:

- Onartutako nabigatzaile luzapenak bakarrik baimenduta
- Aldizka berrikusi eta kendu beharrezkoak ez diren luzapenak
- Jakinarazi luzapenen portaera susmagarria

5.3 Sistema Konfigurazioa

Erabiltzaile Erantzukizunak:

- Ez desgaitu antibirusa edo endpoint babesa
- Ez desgaitu eguneratze automatikoak
- Ez aldatu suebaki ezarpenak
- Ez saiatu pribilegio altuak lortzen (pribilegio eskalatzea)
- Ez manipulatu segurtasun kontrolak edo erregistroak

Administratzaile Sarbidea:

- Administratzaile eskubideak negozio beharra justifikatuta dagoenean bakarrik ematen dira
- Administratzaile kontu bereizia pribilegiatutako zereginetarako (ez eguneroko erabilerarako)
- Administratzaile sarbidea erregistratu eta aldizka berrikusten da
- Aldi baterako administratzaile sarbidea epe zehatz baten ondoren iraungitzen da

5.4 USB Unitateak eta Kanpo Euskarriak

Murrizketak:

- USB unitateak enkriptatuta egon behar dira (enpresak emandako unitate enkriptatuak)
- Eskaneatu kanpo euskarri guztiak antibirusarekin erabili aurretik
- Ez erabili USB unitate pertsonalak enpresaren datuetarako
- Ez konektatu ezezagunak edo ez-fidagarriak diren USB gailuak

Debekatuta:

- Leku publikoetan aurkitutako USB unitateak (balizko eraso bektorea)
- Baimenik gabeko kanpo disko gogorrak
- Baimenik gabe idazteko moduko euskarri optikoak

Salbuespenak: CISOren baimenarekin negozio behar zehatzetarako onartuak

---

6. Posta Elektronikoa eta Komunikazioa

6.1 Posta Elektroniko Erabilera

Erabilera Onargarria:

- Negozio komunikazioak bezeroekin, hornitzaileekin, lankideekin
- Kanpo komunikazio profesionalak
- Erabilera pertsonal mugatua (laburra, ez-komertziala)

Debekatutako Erabilera:

- Eduki iraingarria, jazarlea edo diskriminatzailea bidaltzea
- Spam edo eskatu gabeko mezu masiboak
- Kate gutunak edo piramide eskemak
- Merkataritza jarduera pertsonala (ondasunak/zerbitzuak saltzea)
- Enpresaren posta elektronikoa erabiliz negozioz kanpoko posta zerrendetan harpidetzea
- Besteak ordezkatzea

Posta Elektroniko Segurtasuna:

- Kontuz ibili phishing mezuekin (egiaztatu bidaltzailea estekak klikatu aurretik)
- Ez ireki ustekabeko eranskinak, batez ere bidaltzaile ezezagunengandik
- Egiaztatu diru transferentzia edo kredentzial aldaketa eskaerak (deitu eskatzaileari)
- Jakinarazi mezu susmagarriak security@zabalagailetak.com helbidera
- Erabili [KANPOKOA] adierazlearen kontzientzia (kanpoko mezuak automatikoki etiketatuta)

Informazio Konfidentziala:

- Enkriptatu Konfidentziala edo Oso Konfidentziala den datuak dituzten mezuak
- Egiaztatu hartzaileen helbideak informazio sentikorra bidali aurretik
- Erabili BCC kanpoko mezu masiboetarako (hartzailearen pribatutasuna babestu)
- Ez bidali pasahitzak edo kredentzial sentikorrak posta elektronikoz

Datu Galera Prebentzioa (DLP):

- DLP automatikoak irteerako posta elektronikoa eskaneatzen du
- Kreditu txartel zenbakiak, SSNak edo PII masiboa duten mezuak blokeatu egiten dira
- Politika urraketek segurtasun taldeari alertak sortzen dizkiete

6.2 Posta Elektroniko Atxikipena

- Negozio mezuak Datuen Atxikipen Egutegiaren arabera gordetzen dira
- Erabiltzaileek ez dituzte ezabatu behar lege atxikipenarekin edo ikerketekin lotutako mezuak
- Mezu pertsonalak gutxienekoak izan behar dira eta argi markatu (gaia: [PERTSONALA])
- Artxibatze automatikoa urte baten ondoren artxibo sistemara

6.3 Berehalako Mezularitza eta Kolaborazio Tresnak

Onartutako Tresnak:

- Slack (enpresako lan-eremua)
- Microsoft Teams (M365 tenant)
- Bideo konferentzia: Zoom, Microsoft Teams

Debekatutako Tresnak:

- Negozio komunikazioetarako mezularitza aplikazio pertsonalak (WhatsApp, Telegram, Slack pertsonala)
- Baimenik gabeko kolaborazio plataformak
- Kontsumo mailako fitxategi partekatzea (Dropbox pertsonala, WeTransfer)

Erabilera Jarraibideak:

- Tonu profesionala negozio komunikazioetan
- Ez partekatu informazio konfidentziala kanal publikoetan
- Suposatu mezu guztiak erregistratu eta berrikusi daitezkeela
- Erabili mezu pribatu/zuzenak gai sentikorretarako

---

7. Interneta eta Web Nabigazioa

7.1 Internet Erabilera Onargarria

Baimenduta:

- Negozio ikerketa eta informazio bilketa
- Garapen profesionala eta prestakuntza
- Bezeroekin eta negozio bazkideekin komunikazioa
- Erabilera pertsonal laburra atsedenaldietan (lan orduz kanpo)

Debekatuta:

- Legez kanpoko, iraingarria edo desegokia den edukira sartzea:
    - Helduentzako/pornografia edukia
    - Gorroto hizkera edo eduki estremista
    - Joko guneak (legezko negozio ikerketa ez bada)
    - Legez kanpoko droga edo arma salmenta
    - Hacking, cracking edo pirateria guneak
- Gehiegizko erabilera pertsonala lan orduetan
- Banda zabalera handiko jarduerak (bideo/musika streaming, jokoak) lan orduetan
- Enpresaren politikak edo Espainiako legea urratzen duen edozer

7.2 Web Iragazketa

- Web iragazketa sare korporatiboan eta VPNan behartzen da
- Blokeatutako kategoriak erregistratu eta berrikusten dira
- Blokeatutako edukira sartzeko saiakera errepikatuak ikertzen dira
- Negozio salbuespenak IT bidez eskatu daitezke (justifikazioarekin)

7.3 Sare Sozialak

Sare Sozial Pertsonalak:

- Sare sozial pertsonalen erabilera lan orduetan gutxienekoa izan behar da
- Ez ezagutarazi enpresaren informazio konfidentziala
- Ez hitz egin Zabala Gailetak-en izenean baimenik gabe
- Iritzi pertsonalak argi eta garbi pertsonal gisa identifikatu behar dira (ez enpresaren iritziak)
- Errespetatu lankideen pribatutasuna (ez argitaratu argazkirik baimenik gabe)
- Mantendu ospe profesionala (jokabide desegokiak enpresari eragiten dio)

Enpresaren Sare Sozialak:

- Enpresaren sare sozial ofizialak Marketin taldeak bakarrik kudeatzen ditu
- Langileek enpresaren argitalpen ofizialak partekatu ditzakete
- Etiketatu @ZabalaGailetak (aplikagarria bada) enpresaz publikoki eztabaidatzean
- Krisi komunikazioak: Utzi CEO/Marketinaren esku (ez espekulatu)

Gizarte Ingeniaritza Kontzientzia:

- Kontuz ibili ezezagunen konexio eskaerekin
- Ez partekatu enpresaren informazio sentikorra sare sozialetan
- Adi egon informazio bilketa saiakerekin (lehiakortasun inteligentzia)

---

8. Gailu Mugikorrak eta Urruneko Sarbidea

8.1 Gailu Mugikorrak (Smartphoneak, Tabletak)

Enpresaren Jabetzako Gailuak:

- Enpresaren politika guztien menpe
- Gailu Mugikorren Kudeaketan (MDM) izena eman behar da
- Gailu pasakodea erabili behar da (gutxienez 6 digitu edo baliokidea)
- Enkriptatzea gaitu behar da
- Urruneko garbiketa gaitasuna gaitu behar da
- Enpresak onartutako aplikazioak soilik instalatu behar dira
- Galdutako/lapurtutako gailuak berehala jakinarazi behar dira (segurtasun taldeak urrunetik garbituko du)

Zure Gailua Ekarri (BYOD):

- Gailu pertsonalek enpresaren posta elektronikora sarbidea izan dezakete baimenarekin
- MDMn izena eman behar da (edukiontzi ikuspegia - enpresaren datuak bereizita)
- Gutxieneko segurtasun baldintzak bete behar ditu:
    - Gailu pasakodea gaituta
    - Sistema eragilea eguneratuta
    - Enkriptatzea gaituta
- Enpresak eskubidea du enpresaren datuak urrunetik garbitzeko (ez datu pertsonalak)
- BYOD gailuak ikuskapenaren menpe daude segurtasun intzidente bat susmatzen bada

Gailu Mugikorren Segurtasuna:

- Ez egin jailbreak edo root gailuei
- Instalatu aplikazioak soilik denda ofizialetatik (Google Play, Apple App Store)
- Berrikusi aplikazio baimenak instalatu aurretik
- Ez konektatu konfiantzarik gabeko WiFi-ra VPN gabe
- Kontuz “shoulder surfing”-arekin leku publikoetan

8.2 Urruneko Sarbidea eta VPN

VPN Beharrezkoa Da:

- Enpresaren barne baliabideetara urrunetik sartzeko
- Etxetik edo leku publikoetatik lan egiteko
- Konfiantzarik gabeko WiFi sareetara konektatzeko

VPN Erabilera:

- Erabili enpresak emandako VPN bakarrik (OpenVPN, Cisco AnyConnect)
- Ez erabili VPN zerbitzu pertsonalik (trafikoa ezkutatzen du segurtasun monitorizaziotik)
- Ez partekatu VPN kredentzialak
- Deskonektatu VPNa enpresaren baliabideak erabiltzen ez direnean (errendimendua)

Urruneko Lan Segurtasuna:

- Etxeko WiFi segurua (WPA3 edo WPA2, pasahitz sendoa)
- Etxeko bulegoaren segurtasun fisikoa (dokumentuak, gailuak giltzapetu)
- Familiako kideek ez dute enpresaren gailurik erabili behar
- Bideo dei atzealde kontzientzia (informazio konfidentzialik ez ikusgai)

WiFi Publikoa:

- Saihestu WiFi publikoa lan sentikorretarako ahal bada
- Beti erabili VPNa WiFi publikoan
- Desgaitu WiFi sareetara konektatzeko automatismoa
- Egiaztatu WiFi sarearen legitimitatea (galdetu tokiko langileei)

---

9. Datuen Sailkapena eta Kudeaketa

9.1 Datuen Sailkapena

Informazio guztia Datuen Sailkapen Politikaren arabera sailkatu behar da:

- **Publikoa:** Murrizketarik gabe
- **Barnekoa:** Barne erabilera soilik
- **Konfidentziala:** Sarbide mugatua, negozio eragina ezagutarazten bada
- **Oso Konfidentziala:** Negozio eragin larria, kontrol zorrotzak

9.2 Kudeaketa Baldintzak

Konfidentziala eta Oso Konfidentziala Datuak:

- Enkriptatu gordetzean edo transmititzean
- Sarbide kontrola - jakiteko beharraren arabera
- Markatu dokumentuak sailkapen etiketarekin
- Ez bidali posta elektroniko pertsonaleko kontuetara
- Ez gorde gailu pertsonaletan edo baimenik gabeko hodeiko zerbitzuetan
- Txikitu paperezko dokumentuak bota aurretik
- Jakinarazi galera edo baimenik gabeko ezagutaraztea berehala

Bezeroen Datuak (PII):

- GDPR eta datuen babes politiken menpe
- Lan eginkizunetarako beharrezkoa denean soilik sartu
- Ez kopiatu gailu edo kontu pertsonaletara
- Ez partekatu baimenik gabeko hirugarrenekin
- Jakinarazi datu-urraketak berehala (ordubeteko epean)

Datu Biltegiratzea:

- Gorde negozio datuak onartutako enpresa sistemetan:
    - Fitxategi zerbitzaria (lokala)

        - OneDrive for Business (M365)
        - SharePoint (M365)
        - AWS S3 (aplikazio datuetarako)
- Ez gorde enpresaren datuak hemen:
    - Hodeiko biltegiratze pertsonala (Dropbox pertsonala, Google Drive, iCloud)
    - USB unitate pertsonalak (enpresak emandako enkriptatuak izan ezik)
    - Ordenagailu pertsonalak (MDM duen BYOD onartua izan ezik)

9.3 Datu Transmisioa

Posta Elektronikoa:

- Enkriptatu Konfidentziala/Oso Konfidentziala datuak dituzten mezuak
- Erabili fitxategi transferentzia segurua fitxategi handietarako (ez email eranskinak >25 MB)

Fitxategi Partekatzea:

- Onartua: OneDrive/SharePoint partekatzea iraungitze eta pasahitzekin
- Debekatua: Kontsumo fitxategi partekatzea (WeTransfer, Dropbox esteka pertsonalak)

Euskarri Aldagarriak:

- Erabili USB unitate enkriptatuak (enpresak emandakoak)
- Eskuz eramatea hobesten da posta/mezularitza baino datu oso sentikorretarako

---

10. Hodeiko Zerbitzuak eta Hirugarrenen Aplikazioak

10.1 Onartutako Hodeiko Zerbitzuak

IT-k Onartutako Zerbitzuak:

- Microsoft 365 (emaila, OneDrive, SharePoint, Teams)
- AWS (aplikazio ostalaritza)
- GitHub Enterprise (kode biltegia)
- Slack (talde komunikazioa)
- Zoom (bideo konferentzia)

Onarpena Beharrezkoa:

- Hodeiko zerbitzu berri orok IT eta CISO onarpena behar du
- Hornitzailearen segurtasun ebaluazioa beharrezkoa
- Datuak Tratatzeko Akordioa (DPA) datu pertsonalak kudeatzen dituzten zerbitzuetarako

10.2 Debekatutako Hodeiko Zerbitzuak

Shadow IT Debekatuta:

- Ez erabili baimenik gabeko hodeiko zerbitzuak negozio datuetarako
- Debekatutako zerbitzuen adibideak:
    - Dropbox pertsonala, Google Drive, iCloud enpresaren datuetarako
    - Kontsumo fitxategi partekatzea (WeTransfer, Jumpshare)
    - Proiektu kudeaketa tresna pertsonalak (Trello, Asana) enpresaren datuekin
    - AI zerbitzu pertsonalak (ChatGPT, Claude) enpresaren datu konfidentzialekin

Arriskuak:

- Datu galera (babeskopiarik ez, kontu itxiera)
- Segurtasun ahultasunak
- Betetze urraketak (datuen kokapena, tratamendu akordioak)
- IT laguntza edo monitorizaziorik ez

Salbuespen Prozesua:

- Bidali hodeiko zerbitzu eskaera IT-ri
- Eman negozio justifikazioa
- IT-k segurtasun berrikuspena egiten du
- CISO onarpena beharrezkoa datu sentikorretarako

---

11. Jabetza Intelektuala eta Copyright

11.1 Enpresaren Jabetza Intelektuala

Babesa:

- Enpresaren baliabideak erabiliz sortutako lan produktu guztiak Zabala Gailetak-enak dira
- Merkataritza sekretuak (errezetak, prozesuak) babestu behar dira
- Ez ezagutarazi informazio jabeduna kanpoan NDA eta onarpenik gabe
- Ez kendu dokumentu konfidentzialak instalazioetatik baimenik gabe

Konfidentzialtasuna:

- Mantendu konfidentzialtasuna enpleguan zehar eta ondoren
- Erreferentzia egin Enplegu Kontratuari eta Konfidentzialtasun Hitzarmenari

11.2 Hirugarrenen Jabetza Intelektuala

Copyright Errespetatu:

- Ez deskargatu edo partekatu pirata softwarea, musika, filmak, liburuak
- Lortu lizentzia egokiak erabilitako software eta eduki guztietarako
- Errespetatu kode irekiko lizentziak (bete lizentzia baldintzak)

Software Lizentziak:

- Erabili lizentzia egokia duen softwarea soilik
- Ez gainditu lizentzia kopurua edo esparrua
- Ez partekatu lizentzia gakoak kanpoan

Stock Multimedia:

- Erabili lizentziadun stock argazkiak/musika (enpresaren harpidetzak)
- Aitortu Creative Commons lanak behar den moduan
- Ez erabili copyrightdun materiala baimenik gabe

---

12. Intzidente Jakinarazpena

12.1 Segurtasun Intzidenteak

Berehala Jakinarazi:

- Ustezko malware infekzioa
- Phishing emailak (birbidali security@zabalagailetak.com helbidera)
- Galdutako edo lapurtutako gailuak
- Baimenik gabeko sarbidea kontuetara edo sistemetara
- Datu-urraketak edo ustezko datu galera
- Jarduera susmagarria edo politika urraketak

Jakinarazpen Kanalak:

- Emaila: security@zabalagailetak.com
- Telefonoa: +34 XXX XXX XXX (24/7 telefonoa)
- Aurrez aurre: CISO edo IT Kudeatzailea
- Anonimoa: Segurtasun intzidente web inprimakia

Ez Egin:

- Saiatu zeure kabuz ikertzen (ebidentzia suntsitu dezake)
- Eztabaidatu intzidentea publikoki (mantendu konfidentzialtasuna)
- Atzeratu jakinarazpena (denbora kritikoa da eusterako)

12.2 Politika Urraketak

Jakinarazpena:

- Jakinarazi behatutako politika urraketak honako hauei:
    - Zuzeneko kudeatzailea
    - HR Kudeatzailea
    - CISO
    - Etika telefono anonimoa
- Txistularien babesak aplikatzen dira (errepresaliarik ez)

Ikerketa:

- Txosten guztiak konfidentzialki ikertzen dira
- Urratzaileak diziplina ekintzen menpe daude
- Urraketa errepikatuak edo larriak kaleratzea ekar dezakete

---

13. Produkzio Ingurunea eta OT Sistemak

13.1 OT Sistemako Sarbidea

Sarbide Mugatua:

- Produkzio sistemetara (PLCak, SCADA) sarbidea baimendutako langileei mugatua
- Autentifikazio bereizia IT sistemetatik
- Sarbide fisikoaren kontrola produkzio solairura

Aldaketa Kudeaketa:

- OT sistema aldaketa guztiek aldaketa eskaera eta onarpena behar dute
- Probak beharrezkoak dira produkzio inplementazioaren aurretik
- Konfigurazioen babeskopia aldaketen aurretik
- Dokumentatu aldaketa guztiak

13.2 Produkzio Solairuko Gailuak

Tableta Industrialak eta HMIak:

- Produkzio monitoreorako eta kontrolerako soilik erabiltzen dira
- Erabilera pertsonalik ez
- USB unitaterik ez espresuki baimendu ezean
- Jakinarazi edozein anomalia berehala

Segurtasuna (Safety):

- IT segurtasunak ez du segurtasun (safety) sistemarik arriskuan jarri behar
- Segurtasun sistemak saretik independenteak
- Larrialdi gelditze sistemak beti funtzionalak

---

14. Betetzea eta Legea

14.1 Lege Betetzea

Erabiltzaileek Bete Behar Dituzte:

- Espainiako Zigor Kodea (informatika delituak, datu babesa)
- GDPR (EB 2016/679) eta DBLO-GDD (Espainiako 3/2018 Lege Organikoa)
- Jabetza intelektualaren legeak (copyright, markak, patenteak)
- Enplegu legea eta lan hitzarmenak
- Industria araudiak (elikagaien segurtasuna - zeharka datuen osotasunari eragiten dio)

Debekatutako Legez Kanpoko Jarduerak:

- Hacking edo baimenik gabeko sistema sarbidea
- Datu lapurreta edo espioitza
- Iruzurra edo bidegabeko jabetzea
- Jazarpena edo diskriminazioa
- Edozein jarduera kriminal

14.2 Aurkikuntza Elektronikoa eta Lege Atxikipena

Babes Betebeharrak:

- Lege atxikipena (legal hold) jaulkitzen denean, ez ezabatu edo aldatu zehaztutako datuak
- Lege atxikipenak Aholkulari Juridikoak komunikatzen ditu
- Urraketek lege zigorrak eta kaleratzea ekar ditzakete
- IT-k atxikipen teknikoak ezarriko ditu ahal den neurrian

14.3 Arau Auditoriak

Lankidetza:

- Lankidetzan aritu barne eta kanpo auditoriekin
- Eman informazio zehatza eta osoa
- Ez oztopatu edo engainatu auditoreak

---

15. Monitorizazioa eta Betearazpena

15.1 Monitorizazioa

Zabala Gailetak-ek IT baliabideen erabilera monitorizatzen du honakoetarako:

- Politika betetzea ziurtatzeko
- Segurtasun intzidenteak detektatzeko
- Jokabide okerrak ikertzeko
- Lege betebeharrak betetzeko
- Sistema errendimendua mantentzeko

Monitorizazioak Barne Hartzen Du:

- Sare trafikoaren analisia
- Suebaki eta IDS/IPS log-ak
- Autentifikazio eta sarbide log-ak
- Posta elektronikoaren metadatuak eta edukia (justifikatuta dagoenean)
- Web nabigazio historia
- Fitxategi sarbidea eta aldaketak
- Endpoint segurtasun alertak

Monitorizazio Printzipioak:

- Negozio beharrarekiko proportzionala
- Espainiako lan legearekin bat (Langileen Estatutua)
- Langileen pribatutasuna errespetatzen da ahal den neurrian
- Argi eta garbi pertsonal gisa markatutako komunikazioak babestuta daude
- Baimendutako langileek bakarrik egiten dute monitorizazioa
- Emaitzak konfidentzialki gordetzen dira (jakiteko beharraren arabera partekatzen dira soilik)

15.2 Betearazpena

Urraketa Larritasuna:

Urraketa Txikiak (lehen arau-haustea edo arduragabekeria):

- Adibideak: Pasahitz ahula, zaindu gabeko lan-estazioa, software pertsonala instalatzea
- Ekintza: Ahozko ohartarazpena, berriro prestatzea

Urraketa Larriak (errepikatuak edo nahita egindakoak):

- Adibideak: Pasahitzak partekatzea, baimenik gabeko softwarea, politika ez betetzea ohartarazpenaren ondoren, gehiegizko erabilera pertsonala
- Ekintza: Idatzizko ohartarazpena, sarbide murrizketa, errendimendua hobetzeko plana

Urraketa Oso Larriak (nahita edo legez kanpokoak):

- Adibideak: Datu lapurreta, hacking, malware banaketa, legez kanpoko edukia, jazarpena, iruzurra
- Ekintza: Berehalako etenaldia edo kaleratzea, lege jazarpena, erantzukizun finantzarioa

Diziplina Prozesua:

1. Ikerketa (gertaerak bilatzea, ebidentzia bilketa)
2. Langilearen jakinarazpena eta erantzuteko aukera
3. HR eta zuzendaritzaren erabakia
4. Dokumentazioa langilearen fitxategian
5. Errekurtso prozesua eskuragarri (lan legearen arabera)

Diziplina ekintza guztiak Espainiako lan legearekin eta hitzarmen kolektiboekin bat datoz.

---

16. Prestakuntza eta Kontzientziazioa

16.1 Derrigorrezko Prestakuntza

Langile Berriak:

- AUP prestakuntza lehen astean (ordu 1)
- Aitorpen inprimakia sinatu sistema sarbidea eman aurretik

Langile Guztiak:

- Urteroko freskatze prestakuntza (30 minutu)
- Urteroko politika aitorpena
- Phishing simulazio prestakuntza (hiruhilero)

16.2 Prestakuntza Espezializatua

Garatzaileak:

- Kodeketa seguru praktikak
- Datuen kudeaketa baldintzak

Administratzaileak:

- Pribilegiatutako sarbide erantzukizunak
- Monitorizazioa eta intzidente erantzuna

Kudeatzaileak:

- Betearazpen erantzukizunak
- Intzidente jakinarazpen prozedurak

---

17. Politika Berrikuspena eta Eguneraketak

Berrikuspen Maiztasuna: Urtero edo honako kasuetan:

- Aldaketa teknologiko esanguratsuak
- Lege/arau betekizun berriak
- Segurtasun intzidente handiak
- Antolakuntza aldaketak

Komunikazioa:

- Politika eguneraketak langile guztiei jakinarazten zaizkie
- Aldaketa esanguratsuek berriro aitortzea eskatzen dute
- Enpresaren intraneten eta ISMS atarian eskuragarri

---

18. Salbuespenak

Salbuespen Prozesua:

1. Bidali salbuespen eskaera CISOri
2. Eman negozio justifikazioa
3. Arrisku ebaluazioa egin
4. Konpentsazio kontrolak identifikatu
5. CISO eta dagokion kudeatzailearen onarpena beharrezkoa
6. Salbuespenak denbora mugatuak (gehienez 6 hilabete) eta dokumentatuak

Ohiko Salbuespenak:

- Proiektu zehatzetarako software espezializatua
- Aldi baterako pribilegio altuak
- Ikerketarako blokeatutako guneetara sarbidea

---

19. Aitortza

Erabiltzaile guztiek sinatu behar dute aitorpen hau:

ERABILERA ONARGARRIAREN POLITIKA AITORTZA

Aitortzen dut Zabala Gailetak-en Erabilera Onargarriaren Politika (AUP-001) irakurri, ulertu eta betetzea onartzen dudala.

Ulertzen dut:

- IT baliabideak negozio helburuetarako eskaintzen direla
- Ez dudala pribatutasun itxaropenik enpresaren IT baliabideak erabiltzean
- Nire jarduera monitorizatu eta auditatu daitekeela
- Urraketek diziplina ekintzak ekar ditzaketela, kaleratzea eta lege jazarpena barne
- Nire erabiltzaile kontuaren azpiko jarduera guztien erantzule naizela
- Segurtasun intzidenteak berehala jakinarazi behar ditudala
- Informazio konfidentziala babestu eta jabetza intelektualaren eskubideak errespetatu behar ditudala

IT baliabideak arduraz, profesionalki eta enpresaren politika eta aplikagarria den lege guztien arabera erabiltzea onartzen dut.

Langilearen Izena: _____

Langilearen IDa: _____

Departamentua: _____

Sinadura: _____

Data: _____

Kudeatzailearen Onarpena (sarbidea hornitzeko):

Kudeatzailearen Izena: _____

Sinadura: _____

Data: _____

---

20. Lotutako Politikak eta Dokumentuak

- Informazioaren Segurtasun Politika (ISP-001)
- Pasahitz Politika (PWD-001)
- Datuen Sailkapen Politika
- BYOD Politika
- Urruneko Lan Politika
- Sare Sozialen Politika
- Jokabide Kodea
- Enplegu Kontratua
- Konfidentzialtasun Hitzarmena

---

21. Harremanetarako Informazioa

Politika honi buruzko galderak:

- CISO: ciso@zabalagailetak.com | +34 XXX XXX XXX

IT Laguntza:

- Helpdesk: helpdesk@zabalagailetak.com | +34 XXX XXX XXX

Segurtasun Intzidenteak:

- Segurtasun Taldea: security@zabalagailetak.com | +34 XXX XXX XXX (24/7)

HR Galderak:

- HR Kudeatzailea: hr@zabalagailetak.com | +34 XXX XXX XXX

Politika Urraketak/Etika:

- Telefono Anonimoa: [URL] | +34 XXX XXX XXX

Eranskina A: Erabilera Onargarria Erreferentzia Azkarra

EGIN

✅ Erabili IT baliabideak nagusiki negozio helburuetarako
✅ Babestu zure pasahitzak (sendoak, bakarrak, konfidentzialak)
✅ Blokeatu pantaila mahaia uztean (Windows+L)
✅ Jakinarazi segurtasun intzidenteak berehala
✅ Egiaztatu email bidaltzailea estekak edo eranskinak klikatu aurretik
✅ Enkriptatu datu konfidentzialak partekatzean
✅ Erabili onartutako hodeiko zerbitzuak soilik
✅ Mantendu softwarea eguneratuta
✅ Jarraitu mahai garbiaren politika
✅ Izan profesionala komunikazio guztietan

EZ EGIN

❌ Partekatu zure pasahitza inorekin
❌ Instalatu baimenik gabeko softwarea
❌ Erabili hodeiko biltegiratze pertsonala enpresaren datuetarako
❌ Klikatu email esteka susmagarriak
❌ Desgaitu antibirusa edo segurtasun softwarea
❌ Sartu legez kanpoko edo eduki desegokira
❌ Partekatu informazio konfidentziala kanpoan baimenik gabe
❌ Erabili pirata softwarea
❌ Konektatu WiFi publikora VPN gabe
❌ Utzi gailuak zaintzarik gabe eta desblokeatuta

Eranskina B: Intzidente Jakinarazpen Gida Azkarra

Segurtasun intzidente bat susmatzen baduzu:

1. **GELDITU** - Ez jarraitu arriskuan egon daitekeen jarduerarekin
2. **DESKONEKTATU** - Malwarea susmatzen bada, deskonektatu saretik (ethernet kablea kendu edo WiFi desgaitu)
3. **JAKINARAZI** - Jarri harremanetan segurtasun taldearekin berehala:
    - Emaila: security@zabalagailetak.com
    - Telefonoa: +34 XXX XXX XXX (24/7)
    - Aurrez aurre: CISO bulegoa
4. **GORDE** - Ez ezabatu ezer (ebidentzia behar da)
5. **DOKUMENTATU** - Oharrak hartu gertatutakoaz, noiz, zer behatu duzun

Jakinarazi beharreko ohiko intzidenteak:

- Email susmagarria edo phishing saiakera
- Malware alerta edo ezohiko sistema portaera
- Galdutako edo lapurtutako gailua
- Baimenik gabeko sarbidea kontura
- Ustekabeko datu ezagutaraztea
- USB unitatea edo gailua aurkitzea
- Politika urraketa behatzea

Zalantzarik baduzu, jakinarazi. Hobe seguru egotea damutzea baino. Inor ez da zigortua izango fede onezko jakinarazpenagatik.

Eranskina C: Phishing Alerta Gorriak

Phishing emailen abisu seinaleak:

🚩 Ustekabeko edo eskatu gabeko emaila
🚩 Hizkuntza urgentea edo mehatxagarria (“Ekintza orain!” “Kontua itxiko da!”)
🚩 Bidaltzaile helbide susmagarria (ortografia okerrak, domeinu ezezaguna)
🚩 Agur generikoak (“Kaixo Erabiltzaile” zure izenaren ordez)
🚩 Pasahitzak, kredentzialak edo finantza informazioa eskatzea
🚩 Esteka susmagarriak (pasatu sagua URLaren gainetik - bat dator espero den domeinuarekin?)
🚩 Ustekabeko eranskinak, batez ere .exe, .zip, .scr fitxategiak
🚩 Ortografia eta gramatika txarra
🚩 Egia izateko onegia (loteria irabaziak, ustekabeko itzulketak)

Email susmagarri bat jasotzen baduzu:

1. EZ klikatu estekak edo ireki eranskinak
2. EZ erantzun edo eman informaziorik
3. Birbidali security@zabalagailetak.com helbidera
4. Ezabatu jatorrizko emaila

Legezko eskaerak egiaztatzeko:

- Deitu pertsonari/enpresari zuzenean (erabili ezagutzen duzun telefono zenbakia, ez e-mailekoa)
- Egiaztatu zure kudeatzailearekin edo IT taldearekin ziur ez bazaude
- Bilatu [KANPOKOA] etiketa kanpoko email-etan

ERABILERA ONARGARRIAREN POLITIKAREN AMAIERA