| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P27S | | | | | Naslov dokumenta:<br>**Politika uporabe storitev v oblaku** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>01.01.2025 | | | Lastnik dokumenta: | | | | | | | |
| X | Politika | | Standard | | Postopek | | Obrazec | | Register | | Drugo | |

| **Zgodovina revizij** | | | | |
|---|---|---|---|---|
| **Številka revizije** | **Datum revizije** | **Spremembe** | **Pregledal** | **Lastnik procesa** |
| | | | | |
| | | | | |

| **Odobritve** | | | |
|---|---|---|---|
| **Ime** | **Delovno mesto** | **Datum** | **Podpis** |
| | | | |
| | | | |

Usklajenost s standardi in predpisi

| Standard/predpis | Klavzula/člen | Komentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klavzula 8 | |
| ISO/IEC 27002:2022 | Kontrole 5.23–5.25 | |
| NIST SP 800-53 Rev.5 | AC-20, SC-12, SC-13, SR-5 | |
| Uredba EU GDPR | Člen 28, 32 in poglavje V | |
| Direktiva EU NIS2 | Člen 21(2)(f), (i) | |
| Uredba EU DORA | Člen 5(2), 28 | |
| COBIT 2019 | DSS01, DSS05, BAI04 | |

**1. Namen**

1.1 Ta politika določa, kako se lahko storitve v oblaku varno uporabljajo v organizaciji. Zagotavlja, da so podatki, ki se obdelujejo ali hranijo v oblaku, ustrezno zaščiteni, da je dostop nadzorovan in da se tveganja obvladujejo odgovorno.

1.2 Ta politika malim in srednjim podjetjem pomaga izpolnjevati pravne obveznosti in pričakovanja strank glede varovanja občutljivih informacij, preprečevanja uhajanja podatkov in učinkovitega obvladovanja tveganj, povezanih s storitvami v oblaku, brez potrebe po infrastrukturi na ravni velikih podjetij.

1.3 Ta politika podpira certifikacijo po standardu ISO/IEC 27001, skladnost z GDPR in zanesljivost dobavne verige z doslednim upravljanjem vseh storitev v oblaku, ki jih zagotavljajo tretje osebe.

**2. Področje uporabe**

**2.1 Ta politika se uporablja za:**

2.1.1 vse storitve v oblaku, ki se uporabljajo za hrambo, obdelavo ali prenos podatkov podjetja,

2.1.2 vse zaposlene, pogodbene izvajalce in ponudnike storitev, ki v imenu organizacije uporabljajo orodja v oblaku,

2.1.3 brezplačne in plačljive rešitve v oblaku, vključno s platformami za elektronsko pošto, deljenje dokumentov, orodji SaaS, platformami za varnostno kopiranje, videokonferenčnimi rešitvami in platformami za delo s strankami,

2.1.4 vse naprave (namizne računalnike, mobilne naprave in tablice), ki prek aplikacij v oblaku dostopajo do informacij podjetja.

**2.2 To med drugim vključuje:**

2.2.1 Microsoft 365, Google Workspace, Dropbox Business,

2.2.2 Zoom, Microsoft Teams, Google Meet,

2.2.3 AWS, Azure, GCP,

2.2.4 orodja v oblaku za varnostno kopiranje in obnovitev po nesreči,

2.2.5 deljene mape ali aplikacije, ki se uporabljajo za izdajanje računov, upravljanje projektov ali komunikacijo s strankami.

**3. Cilji**

3.1 Preprečiti nepooblaščeno uporabo neodobrenih storitev v oblaku ali njihovo uporabo z visokim tveganjem.

3.2 Zagotoviti, da so občutljivi ali regulirani podatki, shranjeni v oblaku, zaščiteni z ustreznimi tehničnimi in organizacijskimi kontrolami.

3.3 Določiti jasne vloge za odobritev, konfiguriranje, spremljanje in ukinitev uporabe storitev v oblaku.

3.4 Nadzorovati tokove podatkov ter zagotoviti izpolnjevanje obveznosti glede hrambe, brisanja in zasebnosti za informacije, shranjene v oblaku.

3.5 Zmanjšati odvisnost od osebnih računov ali neevidentiranih orodij tako, da se zahteva odobritev vseh sistemov v oblaku, ki se uporabljajo za legitimne poslovne namene.

3.6 Zagotoviti skladnost z zahtevami standarda ISO/IEC 27001:2022, GDPR, NIS2 in DORA za upravljanje zunanjih odvisnosti od storitev v oblaku.

**4. Vloge in odgovornosti**

**4.1 Generalni direktor**

4.1.1 odobri uporabo vseh novih storitev v oblaku,

4.1.2 pregleda tveganja, povezana s ponudniki storitev v oblaku in vrstami storitev,

4.1.3 zagotavlja izvajanje te politike in odloča o izjemah.

**4.2 Ponudnik IT-podpore ali tehnična podpora**

4.2.1 presodi in uvede varno konfiguracijo storitev v oblaku,

4.2.2 vzpostavi račune, kontrole dostopa in rešitve za varnostno kopiranje,

4.2.3 spremlja skladnost z zahtevami glede gesel, MFA in varnostnih nastavitev.

[ ... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ... ]

**9. Zahteve za pregled in posodobitev**

9.1 To politiko mora generalni direktor v sodelovanju s ponudnikom IT-podpore pregledati najmanj enkrat letno.

**9.2 Formalni pregled je treba izvesti tudi:**

9.2.1 po varnostnem incidentu, povezanem s storitvami v oblaku (npr. kršitev, izguba podatkov),

9.2.2 ob uvedbi nove večje platforme v oblaku,

9.2.3 če se spremenijo pravne ali regulativne zahteve (npr. posodobitve GDPR, NIS2 ali DORA),

9.2.4 če dejavnosti spremljanja odkrijejo neustrezna ravnanja ali nova tveganja.

**9.3 Generalni direktor mora zagotoviti:**

9.3.1 da je evidenca storitev v oblaku posodobljena z novimi ali ukinjenimi storitvami,

9.3.2 da se pravne zahteve in zahteve glede zasebnosti še vedno izpolnjujejo,

9.3.3 da so vse spremembe sporočene ustreznim uporabnikom in zainteresiranim stranem.

9.4 Arhivirane različice morajo biti varno shranjene, stare različice politike pa je treba obravnavati v skladu z organizacijsko P14S – Politika hrambe podatkov in odstranjevanja.

**10. Povezane politike in povezave**

**10.1 To politiko je treba uporabljati usklajeno z naslednjimi politikami informacijske varnosti, prilagojenimi za SME:**

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornost za odobritev storitev v oblaku in upravljanje odnosov s ponudniki.

10.1.2 P4S – Politika nadzora dostopa: podpira varne prijave, upravljanje sej in postopke preklica dostopa, ki so zahtevani za platforme v oblaku.

10.1.3 P14S – Politika hrambe podatkov in odstranjevanja: ureja, kako se podatki v oblaku varnostno kopirajo, hranijo in brišejo v skladu s pravnimi obveznostmi.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da se vsi osebni podatki, shranjeni v storitvah v oblaku, obravnavajo v skladu z načeli GDPR.

10.1.5 P30S – Politika odzivanja na incidente: določa strukturirane postopke za odzivanje na varnostne incidente v oblaku, vključno z zbiranjem dokazov in zunanjim obveščanjem.

10.2 Te politike skupaj zagotavljajo, da je uporaba storitev v oblaku varna, skladna in operativno odporna.

## 11. Referenčni standardi in okviri

### 11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – od organizacij zahteva uvedbo operativnih kontrol za ravnanje s podatki, vključno s tistimi, ki se nanašajo na sisteme v oblaku.

### 11.2 ISO/IEC 27002

11.2.1 Kontrola 5.23 – zahteva upravljanje uporabe storitev v oblaku in orodij SaaS tretjih oseb.

11.2.2 Kontrola 5.24 – zahteva opredeljeno politiko uporabe storitev v oblaku, usklajeno s tveganji in regulativnimi zahtevami.

11.2.3 Kontrola 5.25 – zahteva, da organizacije zagotovijo, da varnostne kontrole v okoljih v oblaku ustrezajo potrebam organizacije.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 AC-20 – zahteva formalne politike uporabe za zunanje sisteme, kot so storitve v oblaku.

11.3.2 SC-12, SC-13 – obravnavata šifriranje podatkov med prenosom in podatkov v mirovanju v okoljih v oblaku.

11.3.3 SR-5 – zajema kontrole tveganj v oblaku in tveganj tretjih oseb v dobavni verigi.

### 11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 28 – zahteva, da ponudniki storitev v oblaku, ki delujejo kot obdelovalci podatkov, spoštujejo zavezujoče pogodbene obveznosti.

11.4.2 Člen 32 – zahteva tehnične in organizacijske kontrole za obdelavo podatkov v oblaku.

11.4.3 Poglavje V – prepoveduje nepooblaščene mednarodne prenose osebnih podatkov, shranjenih v oblaku.

### 11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(f), (i) – zahteva, da bistveni in pomembni subjekti uvedejo ustrezne politike za varnost storitev v oblaku in nadzor dobavne verige.

### 11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 5(2) – zahteva, da finančni subjekti iz segmenta SME vključijo varnost storitev v oblaku v svoje okvire upravljanja tveganj IKT.

11.6.2 Člen 28 – določa pravila nadzora nad kritičnimi zunanjimi ponudniki storitev IKT, vključno s ponudniki storitev v oblaku.

### 11.7 COBIT 2019

11.7.1 DSS01 – »Upravljanje operacij« obravnava operativno celovitost storitev v oblaku.

11.7.2 DSS05 – »Upravljanje varnostnih storitev« vključuje zaščitne ukrepe in spremljanje, značilne za storitve v oblaku.

11.7.3 BAI04 – »Upravljanje razpoložljivosti in zmogljivosti« zagotavlja neprekinjeno poslovanje in zmogljivost v okoljih v oblaku.