ZMH Horvat d.o.o. prepoznaje informaciju kao jedan od svojih najvrjednijih resursa i obvezuje se na njezinu zaštitu od neovlaštenog pristupa, gubitka, izmjene ili zlouporabe. Cilj ove politike je osigurati povjerljivost, cjelovitost i dostupnost podataka te zaštititi osobne, poslovne i druge povjerljive informacije (interna i eksterno primljena) u skladu s važećim zakonodavstvom Republike Hrvatske i Europske unije. **Politika je usklađena s:**
Općom uredbom o zaštiti podataka (EU) 2016/679 (GDPR); Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18); **Zakonom o elektroničkim komunikacijama (NN 76/22)**; **Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)** te smjernicama **EcoVadis "Ethics"** stupa koje zahtijevaju upravljanje povjerljivim informacijama, zaštitu osobnih podataka i prevenciju zlouporabe informacija.

Uprava ZMH Horvat d.o.o. obvezuje se da će:

1) **Osigurati povjerljivost, cjelovitost i dostupnost svih podataka** kojima tvrtka upravlja uključujući osobne, poslovne, tehničke i financijske informacije. Svi zaposlenici imaju pravo anonimno i povjerljivo prijaviti sumnju na povredu informacijske sigurnosti ili zlouporabu podataka putem internog kanala za prijavu nepravilnosti (whistleblowing), bez straha od odmazde.
2) **Primjenjivati načelo "need-to-know"** – pristup informacijama omogućen je isključivo zaposlenicima čije radne obveze zahtijevaju obradu tih podataka.
3) **U slučaju korištenja cloud usluga ili vanjskih informacijskih sustava**, osigurava se da davatelji usluga provode primjerene tehničke i organizacijske mjere zaštite te da se podaci pohranjuju u skladu s GDPR zahtjevima unutar EU/EEA
4) **Zaštititi osobne podatke zaposlenika, kupaca, dobavljača i partnera**, u skladu s GDPR-om i internim procedurama o zaštiti podataka.
5) **Primijeniti fizičke, tehničke i organizacijske mjere zaštite,** uključujući korištenje sigurnih korisničkih lozinki i višefaktorske autentifikacije, ograničeni pristup osjetljivim sustavima, redovite sigurnosne kopije i enkripciju podataka te zaštitu mreža i sustava od zlonamjernih napada. Osigurati sigurnu obradu podataka od strane trećih strana, ugovorima koji definiraju obveze zaštite povjerljivosti i sigurnosti informacija.
6) **Zabraniti neovlašteno otkrivanje, kopiranje, izmjenu, brisanje ili prijenos podataka**, osim ako je to zakonom propisano ili poslovno nužno.
7) **Provoditi redovite edukacije zaposlenika** o pravilima sigurnog rukovanja informacijama, zaštiti osobnih podataka i prepoznavanju cyber-rizika.
8) **Prijaviti svaku povredu sigurnosti podataka** (data breach) bez odgode Voditelju IMS-a i imenovanom Službeniku za zaštitu podataka (DPO), te prema potrebi Agenciji za zaštitu osobnih podataka (AZOP). Uspostavlja se sustav evidencije i izvještavanja o sigurnosnim incidentima te periodični pregled zapisa, s ciljem pravovremenog prepoznavanja prijetnji i provedbe korektivnih mjera.
9) **Osigurati nadzor i praćenje informacijskih sustava** radi prevencije i pravovremenog otkrivanja nepravilnosti.
10) **Kontinuirano poboljšavati sustav informacijske sigurnosti**, u skladu s tehnološkim razvojem, propisima i poslovnim potrebama.

Za provedbu ove politike odgovorni su:

- **Uprava –** strateško upravljanje, odobravanje politike i osiguranje resursa;
- **Voditelj IMS-a** – koordinacija provedbe politike i nadzor nad dokumentacijom**;**
- **Službenik za zaštitu podataka (DPO)** – provedba GDPR obveza i komunikacija s AZOP-om**;**
- **Voditelj tehničkog održavanja** – tehničke mjere zaštite i održavanje sigurnosne infrastrukture**;**
- **Svi zaposlenici** – dužni su pridržavati se pravila i čuvati povjerljivost informacija**.**

Ova politika:

- primjenjuje se na sve djelatnosti, zaposlenike i vanjske suradnike ZMH Horvat d.o.o.
- redovito se revidira najmanje jednom godišnje ili po potrebi, u slučaju promjena zakonodavstva ili tehnologije;
- javno je dostupna i komunicirana svim zaposlenicima i partnerima;
- provodi se kroz dokumentirane postupke i pravila interne kontrole pristupa informacijama.

Ova politika se pohranjuje u sustavu upravljanja dokumentacijom (SOP-IMS-01), objavljuje u internom sustavu komunikacije te se revidira najmanje jednom godišnje ili po potrebi zbog promjena zakonodavstva, tehnologije ili organizacijskih struktura.

U Konjščini, 08.01.2024.; Direktor, Zoran Horvat.

ZMH Horvat d.o.o. recognizes information as one of its most valuable resources and is committed to protecting it from unauthorized access, loss, modification or misuse. The aim of this policy is to ensure the confidentiality, integrity and availability of data and to protect personal, business and other confidential information (internal and externally received) in accordance with the applicable legislation of the Republic of Croatia and the European Union. **The policy is in line with:**

General Data Protection Regulation (EU) 2016/679 (GDPR); Act on the Implementation of the General Data Protection Regulation (NN 42/18); **Electronic Communications Act (NN 76/22); Act on Cybersecurity of Operators of Key Services and Digital Service Providers (NN 64/18) and the EcoVadis "Ethics" pillar** guidelines that require the management of confidential information, the protection of personal data and the prevention of information misuse.

The Management Board of ZMH Horvat d.o.o. undertakes to:

1) **Ensure the confidentiality, integrity and availability** of all data managed by the company, including personal, business, technical and financial information. All employees have the right to anonymously and confidentially report suspected information security breaches or data misuse through the internal whistleblowing channel, without fear of retaliation.
2) **Apply the "need-to-know" principle** where access to information is provided only to employees whose work responsibilities require the processing of such data.
3) **In the case of using cloud services** or external information systems, ensure that service providers implement appropriate technical and organizational protection measures and that data is stored in accordance with GDPR requirements within the EU/EEA.
4) **Protect the personal data of employees,** customers, suppliers and partners, in accordance with GDPR and internal data protection procedures.
5) **Implement physical, technical and organizational security measures**, including the use of secure user passwords and multi-factor authentication, limited access to sensitive systems, regular backups and data encryption, and protection of networks and systems from malicious attacks. Ensure secure data processing by third parties, through contracts that define obligations to protect confidentiality and information security.
6) **Prohibit unauthorized disclosure**, copying, modification, deletion or transfer of data, unless required by law or business necessity.
7) **Conduct regular employee training** on the rules of secure information handling, personal data protection and cyber risk identification.
8) **Report any data security breach without delay to** the Head of IMS and the appointed Data Protection Officer (DPO), and, if necessary, to the Personal Data Protection Agency (AZOP). A system of recording and reporting on security incidents and periodic review of records is established, with the aim of timely identification of threats and implementation of corrective measures.
9) **Ensure supervision and monitoring of information systems** for the purpose of prevention and timely detection of irregularities.
10) **Continuously improve the information security system**, in accordance with technological development, regulations and business needs.

The following are responsible for implementing this policy:

- **Management** – strategic management, policy approval and resource provision;
- **IMS Manager** – coordination of policy implementation and supervision of documentation;
- **Data Protection Officer (DPO)** – implementation of GDPR obligations and communication with AZOP;
- **Technical Maintenance Manager** – technical protection measures and maintenance of security infrastructure;
- **All employees** – are obliged to comply with the rules and maintain the confidentiality of information.

This policy:

- applies to all activities, employees and external collaborators of ZMH Horvat d.o.o.
- is regularly revised at least once a year or as necessary, in the event of changes in legislation or technology;
- is publicly available and communicated to all employees and partners;
- is implemented through documented procedures and rules of internal information access control.

This policy is stored in the document management system (SOP-IMS-01), published in the internal communication system and revised at least once a year or as necessary due to changes in legislation, technology or organizational structures.

In Konjščina, 08.01.2024.; Director, Zoran Horvat.