Mplus BPTO

Politika informacijske sigurnosti

Information Security Policy

Zagreb, 12.Ožujak 2026.

SVRHA

- Svrha Politike informacijske sigurnosti jest zaštita imovine i informacija društva, uključujući osobne podatke i privatnost, od svih vrsta prijetnji – bilo unutarnjih ili vanjskih, namjernih ili nenamjernih.
- Sigurnost pojedinaca i informacijskih sustava od ključne je važnosti za ostvarenje temeljnih ciljeva društva.
- Svrha je osigurati kontinuiranu identifikaciju slabosti, pravovremeno otkrivanje sigurnosnih događaja i incidenata, prilagodbu poslovnim potrebama, usklađenost s važećim propisima te usklađenost s vanjskim i unutarnjim okruženjem.

OVLASTI

- Direktori društva podržavaju i odobravaju politiku informacijske sigurnosti. Cijela politika informacijske sigurnosti temelji se na načelu organizacije projekta društva i izravnoj odgovornosti zaposlenika i ugovornog osoblja.

CILJEVI

- Cilj je osigurati da su informacije dostupne isključivo ovlaštenim osobama (povjerljivost) u trenutku kada su im potrebne (dostupnost).
- Osigurati cjelovitost informacija.
- Cilj je smanjiti učestalost incidenata vezanih uz informacijsku sigurnost te otkloniti nedostatke u sustavu upravljanja informacijskom sigurnošću.

PURPOSE

- The purpose of the Information Security Policy is to protect the group's assets and information, as well as personal data and privacy, from all types of threats, whether internal or external, intentional or unintentional.
- The security of individuals and information systems is of critical importance in supporting the company's fundamental objectives.
- The purpose is to ensure continuous identification of vulnerabilities, timely detection of security events and incidents, alignment with business needs, compliance with applicable regulations, and consistency with both external and internal environments.

AUTHORITIES

- The company directors support and approve the information security policy. The entire information security policy is based on the principle of organizing the company's projects and the direct responsibility of employees and contracted personnel.

GOALS

- To ensure that information is available only to authorized individuals (confidentiality) when they need it (availability).
- To ensure the integrity of information.
- The objective is to reduce the frequency of information security incidents and to address deficiencies within the information security management system.

- Cilj je osigurati usklađenost poslovnih aktivnosti s važećim zakonodavstvom o zaštiti podataka i privatnosti te uspostaviti učinkovit i održiv okvir informacijske sigurnosti unutar društva.

- U okviru ostvarivanja strateških ciljeva društva vezanih uz informacijsku sigurnost, razvijeni su standardi, prakse i postupci te su implementirane odgovarajuće mjere koje podržavaju provedbu Politike informacijske sigurnosti.

- The objective is to ensure that business activities comply with applicable data protection and privacy legislation, and to establish an effective and sustainable information security framework within the organization.

- As part of achieving the company's strategic objectives in information security, standards, practices, and procedures have been developed, and appropriate measures have been implemented to support the enforcement of the Information Security Policy.

ODGOVORNOSTI

- Svaki je zaposlenik odgovoran za poštivanje Politike informacijske sigurnosti i pridržavanje načela Sustava upravljanja informacijskom sigurnošću. Pojedinci podliježu disciplinskim mjerama u slučaju kršenja Politike informacijske sigurnosti ili bilo kojeg elementa sustava upravljanja informacijskom sigurnošću.
- Svi rukovoditelji unutar društva izravno su odgovorni za provedbu Politike informacijske sigurnosti unutar područja svoje odgovornosti te za osiguranje usklađenosti s odredbama politike od strane svojih podređenih.

RESPONSIBILITIES

- Each employee is responsible for complying with the Information Security Policy and adhering to the principles of the Information Security Management System. Individuals are subject to disciplinary action for any violation of the Information Security Policy or any element of the Information Security Management System.
- All managers within the company are directly responsible for implementing the Information Security Policy within their respective areas of responsibility and for ensuring that their subordinates comply with its provisions.

DISTRIBUCIJA

- Politika informacijske sigurnosti komunicira se svim zaposlenicima putem internih komunikacijskih kanala te je dostupna svima putem elektroničke oglasne ploče – Sharepointa – ili u fizičkom obliku.
- Osigurati kontinuiranu komunikaciju sa zaposlenicima o temama vezanim uz informacijsku sigurnost, identifikaciju rizika te primjenu mjera za podizanje svijesti o važnosti sveobuhvatne sigurnosti.

DISTRIBUTION

- The Information Security Policy is communicated to all employees through internal communications and is made available to everyone via the company's electronic notice board – Sharepoint – or in physical form.
- Ensure continuous communication with employees regarding information security, risk identification, and the implementation of measures aimed at raising awareness of the importance of comprehensive security.

- Redovito se upoznavati s pojedinostima uspostavljenog sustava upravljanja, zakonodavnim novostima, aspektima informacijske sigurnosti, izmjenama politika te poduzetim mjerama, kao i s vlastitim odgovornostima u području sigurnosti.

PREGLED I ODRŽAVANJE POLITIKE INFORMACIJSKE SIGURNOSTI

- Upravljanje informacijskom sigurnosti smatra se kontinuiranim procesom koji uključuje planiranje, implementaciju, praćenje i akciju, s kojim neprestano povećavamo razinu sigurnosti informacija.
- Sustav upravljanja informacijskom sigurnošću pregledava se najmanje jednom godišnje, ili češće prema potrebi, samostalno ili u sklopu drugih pregleda, u kontekstu internih revizija.
- Redovito recenzirati Politiku informacijske sigurnosti i procjenjivati njezinu prikladnost tijekom svake evaluacije uprave, najmanje jednom godišnje, te osigurati da se sve značajnije promjene politike upućuju na razmatranje i odobrenje upravi.
- Sve poslovne aktivnosti provode se u skladu s važećim zakonskim propisima relevantnima za poslovanje društva, s posebnim naglaskom na usklađenost s regulativama iz područja informacijske sigurnosti, zaštite osobnih podataka, poslovne tajne te autorskih i licencnih prava.
- Izmjene Politike informacijske sigurnosti provode se prema potrebi, tijekom redovitih pregleda sustava, u slučaju pogrešaka u postojećim procedurama, kao i uslijed promjena poslovnih procesa ili organizacijskih prilagodbi.

PROMJENE

- Promjene Politike informacijske sigurnosti provode se na temelju redovitih evaluacija sustava upravljanja, zakonodavnih novosti, poslovnih potreba te unutarnjih i vanjskih čimbenika koji utječu na sigurnosno

- Regularly become familiar with the details of the established management system, legislative developments, aspects of information security, policy changes, implemented measures, and individual responsibilities in the area of security.

REVIEW AND MAINTENANCE OF THE INFORMATION SECURITY POLICY

- Information security management is considered a continuous process that includes planning, implementation, monitoring, and action, through which we continuously enhance the level of information security.
- The Information Security Management System is reviewed at least once a year, or more frequently, if necessary, either independently or in conjunction with other reviews, within the context of internal audits.
- Regularly review the Information Security Policy and assess its adequacy during each management review, at least once per year, and ensure that all significant policy changes are submitted for management evaluation and approval.
- All business activities are conducted in accordance with applicable legal regulations relevant to the company's operations, particularly regarding compliance with information security, personal data protection, trade secrets, and copyright and licensing rights.
- Changes to the Information Security Policy are implemented as needed, during regular system reviews, or in the event of errors in existing procedures, as well as due to changes in business processes and organizational adjustments.

CHANGES

- Changes to the Information Security Policy are made based on regular reviews of the management system, legislative updates, business requirements, and internal and external factors affecting the security

okruženje.

- Sve promjene dokumentiraju se, komuniciraju relevantnim dionicima te se implementiraju u skladu s definiranim postupkom upravljanja promjenama.

environment.

- All changes are documented, communicated to relevant stakeholders, and implemented in accordance with the defined change management procedure.

12.03.2026

Igor Varivoda, direktor

M Plus BPTO d.o.o.
Zagreb