POLITIKA INFORMACIJSKE SIGURNOSTI

Priroda poslovnih aktivnosti Micro-Link-a uključuje obradu i razmjenu informacija s različitim unutarnjim i vanjskim dionicima, čime im pomažemo u maksimalnom iskorištavanju poslovnih prilika, pretvarajući tehnološke potencijale u stvarne poslovne vrijednosti, u skladu s našim strateškim ciljevima.
Za očuvanje kontinuiteta poslovanja, ključno je poduzimati mjere zaštite informacija i povezane informacijske imovine od svih mogućih prijetnji, bilo unutarnjih ili vanjskih, koje bi mogle ugroziti povjerljivost, integritet i dostupnost podataka.

Kako bi smanjila rizike informacijske sigurnosti i definirala odgovarajuće upravljanje informacijskom sigurnošću, Uprava Micro-Link-a obavezala se na kontinuirano poboljšanje informacijske sigurnosti i osiguranje resursa putem Sustava upravljanja informacijskom sigurnošću uspostavljenog u skladu sa zahtjevima norme ISO/IEC 27001:2022.

Uprava se obvezuje se na osiguranje i održavanje:
- povjerljivosti informacija, te zaštitu od neovlaštenog pristupa ili eventualne zloupotrebe
- cjelovitosti informacija kako bi se osigurala primjenjivost u poslovnom odlučivanju
- dostupnosti informacija i povezane informacijske imovine u svrhu izvršavanju poslovnih obveza.

U svrhu očuvanja povjerljivosti, integriteta i dostupnosti informacija i informacijske imovine, Micro-Link se obvezuje slijediti navedena načela poslovanja:

1. Uspostaviti mjerljive ciljeve i pratiti djelotvornost primijenjenih sigurnosnih mjera s ciljem osiguranja kontinuiranog razvoja i poboljšanja sustava informacijske sigurnosti.
2. Usmjeriti pažnju na izgradnju odnosa i komunikacije s klijentima i dobavljačima uz duboko razumijevanje njihovih potreba i očekivanja u kontekstu našeg poslovanja.
3. Osigurati kontinuirano osvješćivanje i edukaciju zaposlenika u svrhu dosezanja i održavanja visoke razine svijesti i kompetencija u području informacijske sigurnosti.
4. Provoditi redovite analize i procjene sigurnosnih rizika u predviđenim vremenskim okvirima, te tretirati identificirane rizike sukladno poslovnom utjecaju i njihovim prioritetima.
5. Minimizirati prijetnje za redovito poslovanje upravljanjem prepoznatim rizicima.
6. Pravovremeno prepoznati, ograničiti utjecaj i prijaviti svako narušavanje informacijske sigurnosti nadležnim osobama, te istražiti uzroke i poduzeti odgovarajuće mjere za ublažavanje posljedica i sprečavanje ponavljanja.
7. Razviti, održavati i redovito testirati planove za oporavak i kontinuitet poslovanja.
8. Primjenom integriranih sigurnosnih mjera ispuniti sve zakonske, regulatorne i ugovorne zahtjeve, kao i druge specifične zahtjeve u području informacijske sigurnosti na koje se tvrtka Micro-Link obvezala.

Sustav upravljanja informacijskom sigurnošću, zajedno s usvojenom i odobrenom politikom, bit će redovito ažuriran.
Svi zaposlenici, dobavljači i vanjski suradnici Micro-Link-a dužni su pridržavati se zahtjeva propisanih ovom politikom pri radu s informacijskim resursima.

Ova Politika stupa na snagu s datumom donošenja i dostupna je svim zainteresiranim stranama na Internet stranicama Micro-Link-a.

14.04.2025.

MICRO-LINK d.o.o.
Darko Žvan, Član Uprave