Najviše rukovodstvo Termoinženjeringa uspostavlja politiku bezbednosti informacija kojom se obavezuje da će obezbediti i zaštititi kompletnu materijalnu i informacionu imovinu od svih oblika pretnji, internih i eksternih, slučajnih ili namernih, kroz uspostavljanje, primenu, nadzor, preispitivanje, održavanje i poboljšanje sistema upravljanja bezbednošću informacija, a u skladu sa zahtevima standarda ISO 27001.

Sprovođenje ove politike važno je za održavanje integriteta informacionog sistema i imovine preduzeća, kao i bezbednosti imovine korisnika, a u cilju pružanja kvalitetnih usluga korisnicima i drugim zainteresovanim stranama.

Politika obezbeđuje i garantuje:

- poverljivost, integritet i raspoloživost informacija, odnosno njihovu zaštitu od neovlašćenog pristupa, izmene i upotrebe bilo slučajnim ili namernim aktivnostima,
- preventivne mere kojima se sprečava gubljenje ili uništenje podataka organizacije,
- otklanjanje softverskih grešaka, neometan rad servera,
- usaglašenost sa svim regulatornim i zakonskim zahtevima,
- obuku koja se obavlja kroz sve organizacione delove,
- sve povrede sigurnog rukovanja informacijama će se razmatrati, istražiti i dokumentovati.

Ciljevi:

- zaštita podataka korisnika usluga,
- čuvanje poverljivosti u svim slučajevima pristupa dostupnim informacijama,
- zaštita fizičke i informacione imovine organizacije,
- pružanje pouzdanih informacija,
- garantovanje raspoloživosti informacija ovlašćenim osobama.

Rukovodstvo organizacije obezbeđuje da ova politika bude saopštena, razumljiva, implementirana i održavana u organizaciji i najmanje jednom godišnje preispitivana i poboljšavana. Svi zaposleni (stalno ili privremeno), ugovorne strane, konsultanti i ostale zainteresovane strane svesni su svojih obaveza i odgovornosti, a koje su definisane u okviru njihovih poslova i ugovora.

Svi zaposleni moraju da pruže podršku rukovodstvu koje je propisalo politiku i pravila. Posledice nepoštovanja politike bezbednosti su definisane u okviru disciplinskog postupka.