REGOLAMENTO AZIENDALE PER L'USO DEGLI STRUMENTI INFORMATIVI
CONFORME DIRETTIVA NIS2

Code: LOD100416W-0000-00 **File:** LVH0000057003.DOCX **Data:** 17/06/2026

Azienda:	LIVE-TECH Srl
Sede legale:	Via Terzolo n. 19 Alba (CN)
Sede operativa:	Via Stazione n. 65 Monticello d'Alba (CN)
P.IVA / C.F.:	02806620049
Responsabile IT/CISO:	Mauro Luigi Cortese
DPO (Responsabile Protezione Dati):	Domenico Veglio

REGISTRO DELLE REVISIONI

Revisione	Data	Modifiche	Approvato da
00	17/06/2026	Prima emissione	Mauro Luigi Cortese

1 Scopo

Il presente regolamento definisce le regole per un utilizzo corretto, sicuro e conforme degli strumenti informativi aziendali, in linea con la Direttiva NIS2, il GDPR e le best practice di sicurezza.

2 Ambito di applicazione

Il regolamento si applica a tutti gli utenti autorizzati: dipendenti, collaboratori, consulenti e fornitori che accedono ai sistemi informatici aziendali.

3 Classificazione dei dati e degli asset

Le informazioni aziendali sono classificate in: Critiche, Importanti e Standard. Gli utenti devono trattare ogni informazione secondo il livello assegnato.

4 Uso degli strumenti informatici

Gli strumenti sono forniti per scopi lavorativi. È vietato installare software non autorizzato, utilizzare dispositivi personali senza approvazione o aggirare controlli di sicurezza.

5 Gestione accessi e autenticazione

Ogni utente dispone di credenziali personali. È obbligatorio utilizzare password robuste e autenticazione multi- fattore ove prevista. È vietata la condivisione degli account.

6 Sicurezza operativa

Gli utenti devono bloccare le postazioni, mantenere aggiornati i dispositivi e rispettare le politiche di sicurezza. Qualsiasi anomalia deve essere segnalata immediatamente.

7 Gestione degli incidenti

Eventuali incidenti di sicurezza devono essere segnalati tempestivamente al Responsabile IT / CISO. È vietato intervenire autonomamente su eventi critici senza autorizzazione.

Tempi di notifica obbligatori (art. 23 NIS2 / D.lgs. 138/2024):

- **Entro 24 ore:** prenotifica all'Agenzia per la Cybersicurezza Nazionale (ACN) per incidenti significativi.
- **Entro 72 ore:** notifica completa all'ACN e, per violazioni di dati personali, al Garante per la Protezione dei Dati Personali (GDPR art. 33).
- **Entro 1 mese:** relazione finale all'ACN.

8 Utilizzo e-mail e Internet

La posta aziendale e Internet devono essere utilizzati esclusivamente per finalità professionali. È vietato accedere a contenuti non sicuri o diffondere informazioni riservate.

9 Protezione dei dati

I dati aziendali devono essere protetti e archiviati in sistemi autorizzati. È vietata la diffusione non autorizzata di informazioni. I dati sensibili e critici devono essere protetti mediante crittografia sia in transito (TLS/HTTPS) sia a riposo (art. 21 c. 2 lett. h NIS2). In caso di violazione di dati personali, il DPO deve essere informato immediatamente al fine di notificare il Garante entro 72 ore (GDPR art. 33) e, se del caso, gli interessati entro 72 ore dall'accertamento (GDPR art. 34). Per informazioni sui diritti degli interessati (accesso, rettifica, cancellazione) fare riferimento all'Informativa Privacy aziendale.

9.1 Sicurezza della supply chain

In conformità all'art. 21 c. 2 lett. d del D.Lgs. 138/2024 (NIS2), l'azienda valuta e gestisce i rischi di sicurezza derivanti dai fornitori e dai partner della catena di approvvigionamento. I fornitori che accedono ai sistemi aziendali devono rispettare i requisiti minimi di sicurezza definiti contrattualmente. Qualsiasi accesso di terze parti deve essere autorizzato, tracciato e limitato al minimo necessario (principio di minimo privilegio).

10 Lavoro da remoto

È obbligatorio utilizzare VPN aziendale, evitare reti non sicure e garantire la protezione dei dispositivi.

11 Monitoraggio e controlli

L'azienda si riserva il diritto di monitorare l'utilizzo dei sistemi nel rispetto delle normative.

12 Formazione

Gli utenti devono partecipare a corsi di formazione sulla sicurezza informatica e aggiornamenti periodici.

13 Continuità operativa

Gli utenti devono attenersi ai piani di continuità operativa e disaster recovery in caso di emergenza.

14 Violazioni e sanzioni

Le violazioni del regolamento possono comportare sanzioni disciplinari e, nei casi gravi, conseguenze legali.

APPROVAZIONE AZIENDALE

Il presente regolamento è stato approvato dalla Direzione aziendale.

Responsabile IT/CISO	MAURO LUIGI CORTESE
Direzione Generale	DOMENICO VEGLIO
Data e luogo di approvazione	Monticello lì 17/06/2026