OVERMACH
MACCHINE UTENSILI

Classificazione: PUBBLICO

Politica per la sicurezza delle informazioni

Overmach S.p.A. – Rev. 01 del 10/10/2026

1 Scopo e campo di applicazione

La presente Politica definisce i principi e gli impegni con cui Overmach S.p.A. protegge le informazioni, le reti e i sistemi informativi che supportano le proprie attività di commercio, installazione e assistenza di macchine utensili, stampanti 3D e software per l'industria meccanica.

La Politica si applica a tutte le sedi, ai processi e ai sistemi informativi aziendali, a tutto il personale e ai collaboratori, nonché ai fornitori e alle terze parti che accedono a informazioni o sistemi di Overmach o che erogano servizi rilevanti per la continuità delle attività aziendali.

2 Contesto e impegno della Direzione

Overmach S.p.A. rientra tra i soggetti importanti ai sensi del D.Lgs. 138/2024, di recepimento della Direttiva (UE) 2022/2555 (NIS2). La Direzione riconosce la sicurezza delle informazioni come elemento essenziale per la fiducia di clienti, fornitori e collaboratori e per la continuità del business, e si impegna a:

- approvare le misure di gestione dei rischi per la sicurezza informatica e sovrintenderne l'attuazione, come previsto dall'art. 23 del D.Lgs. 138/2024;
- mettere a disposizione le risorse umane, tecniche ed economiche necessarie;
- seguire una formazione periodica in materia di sicurezza informatica e promuoverla a tutti i livelli dell'organizzazione;
- rispettare le leggi e i regolamenti applicabili, in particolare la normativa NIS2, il Regolamento (UE) 2016/679 (GDPR) e gli obblighi contrattuali verso clienti e partner.

3 Principi

Le informazioni aziendali, dei clienti e dei fornitori sono protette secondo tre principi fondamentali:

- **Riservatezza:** le informazioni sono accessibili solo alle persone autorizzate, in base al principio del minimo privilegio e della necessità di conoscere;
- **Integrità:** le informazioni sono accurate e complete e sono protette da modifiche non autorizzate;
- **Disponibilità:** le informazioni e i servizi sono accessibili agli utenti autorizzati quando necessario, anche in caso di incidente.

4 Impegni e misure di sicurezza

In coerenza con l'art. 24 del D.Lgs. 138/2024 e con le specifiche dell'Agenzia per la Cybersicurezza Nazionale, Overmach adotta misure tecniche, operative e organizzative adeguate e proporzionate ai rischi, tra cui:

- **Analisi e gestione dei rischi:** valutazione periodica dei rischi per le reti e i sistemi informativi e definizione di piani di trattamento;
- **Gestione degli incidenti:** rilevazione, gestione e notifica degli incidenti significativi al CSIRT Italia nei tempi previsti dalla legge;

- **Continuità operativa:** backup, ripristino in caso di disastro e gestione delle crisi per garantire la continuità dei servizi;
- **Sicurezza della catena di approvvigionamento:** qualifica dei fornitori ICT e critici, clausole di sicurezza contrattuali e monitoraggio dei rischi legati alle terze parti;
- **Sicurezza dei sistemi:** acquisizione, sviluppo, configurazione e manutenzione sicura di reti e sistemi, con gestione delle vulnerabilità e degli aggiornamenti;
- **Controllo degli accessi:** gestione delle identità, autenticazione a più fattori ove opportuno, revisione periodica delle utenze e dei privilegi;
- **Gestione degli asset e crittografia:** inventario degli asset informatici e uso di tecniche crittografiche per la protezione dei dati;
- **Igiene informatica e formazione:** pratiche di base di sicurezza e formazione periodica di tutto il personale sui rischi informatici;
- **Verifica dell'efficacia:** controlli periodici sull'efficacia delle misure adottate e miglioramento continuo.

5 Ruoli e responsabilità

- **Direzione:** approva la Politica e le misure di sicurezza, ne verifica l'attuazione e ne risponde ai sensi della normativa.
- **Chief Information Security Officer (CISO):** coordina il sistema di gestione della sicurezza, la valutazione dei rischi e la gestione degli incidenti; è il Punto di Contatto verso l'Agenzia per la Cybersicurezza Nazionale.
- **Personale e collaboratori:** rispettano la Politica e le procedure aziendali, proteggono le credenziali e le informazioni loro affidate e segnalano tempestivamente eventi sospetti.
- **Fornitori e terze parti:** rispettano i requisiti di sicurezza contrattuali e comunicano senza ritardo gli incidenti che possono avere impatto su Overmach.

6 Comunicazione e riesame

La Politica è comunicata a tutto il personale, resa disponibile alle parti interessate e pubblicata sul sito www.overmach.it. È riesaminata almeno una volta l'anno e in occasione di cambiamenti significativi del contesto, dell'organizzazione, delle minacce o della normativa. Eventuali violazioni della Politica sono gestite secondo le procedure aziendali e i contratti in essere.