

POLITICA DEL SISTEMA DI GESTIONE INTEGRATO PER LA QUALITÀ, LA SALUTE, LA SICUREZZA DEI LAVORATORI, L'AMBIENTE e LA CYBERSECURITY

Concetti S.p.A. svolge attività di **progettazione, costruzione, assemblaggio ed installazione di macchine ed impianti per insacco e palettizzazione; erogazione di servizi di assistenza, manutenzione e riparazione di impianti e macchine.**

Le attività di progettazione e produzione vengono svolte nella sede sita in Via della Comunità 14, fraz. Ospedalichio di Bastia Umbra.

L'Organizzazione si impegna a:

- garantire un ambiente di lavoro sicuro e salubre per i propri dipendenti, collaboratori e visitatori;
- ridurre il proprio impatto ambientale;
- fornire ai clienti un prodotto della massima affidabilità;
- un livello di servizio estremamente elevato;
- un miglioramento continuo dei processi e dei prodotti;
- il rispetto delle leggi e normative vigenti per il servizio;
- l'efficienza operativa dei processi.

Nello specifico, l'Organizzazione istituisce e mantiene attivo un Sistema di Gestione conforme ai seguenti riferimenti giuridici e norme tecniche volontarie nazionali ed europee:

- ISO 9001:2015
- ISO 14001:2015
- ISO 45001:2023
- Direttiva 2014/32/UE
- Direttiva 2006/42/CE / Regolamento UE 2023/1230
- D. Lgs 231/2001 e s.m.i.
- D. Lgs. 81/2008 e s.m.i.
- D. Lgs 152/2006 e s.m.i.
- Regolamento 2016/679 GDPR

L'Organizzazione si impegna inoltre a garantire la conformità alle normative vigenti inerenti alla cybersecurity (NIS2).

Il nostro impegno si traduce nell'adozione di un approccio sistematico e strutturato alla gestione della qualità, della sicurezza sul lavoro e della tutela ambientale, garantendo il miglioramento continuo delle prestazioni attraverso obiettivi chiari e misurabili.

Obiettivi e Principi

1. **Conformità Normativa:** Assicuriamo il rispetto delle leggi e regolamenti applicabili in materia di qualità, sicurezza, salute sul lavoro e ambiente, cybersecurity, nonché degli altri requisiti sottoscritti dall'organizzazione. Ci impegniamo a mantenere un aggiornamento costante rispetto alle normative vigenti e a garantire la loro applicazione efficace all'interno della nostra realtà aziendale.

Il sistema di gestione della sicurezza informatica copre tutti i processi aziendali, inclusi progettazione, produzione, installazione e assistenza, nonché i sistemi informativi e le infrastrutture di rete a supporto.

2. **Miglioramento Continuo:** Implementiamo e miglioriamo costantemente il nostro Sistema di Gestione, adottando strategie di prevenzione per ridurre il numero di incidenti sul lavoro, malattie professionali e impatti ambientali negativi, e per aumentare la qualità dei nostri prodotti e servizi. L'Organizzazione si impegna a garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi aziendali, attraverso l'adozione di misure tecniche, organizzative e procedurali adeguate al livello di rischio. Ci impegniamo anche a porre in essere strategie per evitare incidenti di cybersecurity. Monitoriamo regolarmente le nostre prestazioni tramite audit interni, analisi dei dati e revisioni periodiche.

3. **Soddisfazione del Cliente:** Poniamo il cliente al centro delle nostre attività, garantendo un servizio che soddisfi o superi le sue aspettative. Monitoriamo il grado di soddisfazione attraverso feedback e indagini, adottando azioni di miglioramento quando necessario.

4. **Prevenzione dei Rischi:** Identifichiamo, valutiamo e gestiamo i rischi per la salute e la sicurezza dei lavoratori, riducendo al minimo le esposizioni a potenziali pericoli. In ambito ambientale, ci impegniamo

a individuare e mitigare i rischi connessi alle nostre attività, promuovendo tecnologie e processi a basso impatto.

Le fasi di valutazione e gestione dei rischi sono estesi anche alla cybersecurity, nel cui ambito ci impegniamo a mitigare i rischi rilevati, nonché a mitigarne l'impatto nel momento in cui si dovessero verificare.

5. **Partecipazione e Consultazione:** Coinvolgiamo attivamente i lavoratori e i loro rappresentanti nei processi decisionali relativi alla qualità, sicurezza e ambiente, promuovendo una cultura della prevenzione e dell'eccellenza. Favoriamo la segnalazione di situazioni a rischio e incentiviamo la collaborazione attraverso incontri periodici, formazione e programmi di sensibilizzazione.

Per la cybersecurity, l'azienda aderisce anche alle procedure e utilizza i sistemi di segnalazione degli incidenti imposti dalla Agenzia di Cybersecurity Nazionale (ACN)

6. **Uso Responsabile delle Risorse:** Adottiamo misure per ottimizzare il consumo di energia, acqua e materie prime, promuovendo l'efficienza e riducendo la produzione di rifiuti. Implementiamo politiche di riciclo e riutilizzo, sensibilizzando i dipendenti sulle migliori pratiche per la gestione sostenibile delle risorse.

7. **Gestione delle Emergenze:** Sviluppiamo e aggiorniamo costantemente piani di emergenza per minimizzare i rischi per le persone e per l'ambiente in caso di incidenti o eventi imprevisti. Organizziamo esercitazioni periodiche per verificare l'efficacia delle procedure e garantire una risposta tempestiva e adeguata.

Nel caso specifico di emergenze dovute ad incidenti di cybersecurity, l'Organizzazione garantisce la tempestiva segnalazione degli incidenti di sicurezza informatica secondo le procedure previste dalla Direttiva NIS2 e dalle linee guida dell'ACN.

L'Organizzazione assicura anche la continuità operativa dei servizi critici mediante piani di disaster recovery e ICT continuity, riesaminati e testati periodicamente.

8. **Formazione e Sensibilizzazione:** Garantiamo che tutti i dipendenti e collaboratori ricevano una formazione continua per svolgere il proprio lavoro in sicurezza, garantire il mantenimento dei buoni standard di salute, con consapevolezza ambientale e con competenze adeguate a garantire elevati standard qualitativi. Offriamo corsi specifici su normative, utilizzo di attrezzature, gestione dei rifiuti, controllo qualità e pratiche sostenibili per migliorare il coinvolgimento e la responsabilizzazione del personale.

La formazione è estesa anche all'igiene e sicurezza informatiche, poiché l'Organizzazione riconosce che il personale è normalmente l'anello più vulnerabile della catena di cybersecurity.

9. **Monitoraggio e Controllo:** Eseguiamo audit periodici e monitoraggi per verificare l'efficacia del sistema e l'aderenza agli obiettivi aziendali. Valutiamo gli indicatori di performance e utilizziamo i dati raccolti per apportare miglioramenti concreti e mirati nella qualità dei prodotti e servizi, nella sicurezza e nella gestione ambientale.

La Direzione, in conformità all'art. 23 del D.Lgs. 138/2024 (NIS2), assume la responsabilità diretta della supervisione delle misure di sicurezza informatica e dell'allocazione delle risorse necessarie alla loro attuazione e promuove audit interni e riesame annuale del sistema o in occasione di cambiamenti significativi nel contesto o nei rischi informatici. La sicurezza informatica è estesa ai fornitori critici e ai partner tecnologici, che sono valutati anche per i loro livelli di conformità alle normative di cybersecurity.

Tali obiettivi vengono declinati nelle seguenti strategie a breve, medio e lungo termine.

Gli obiettivi specifici per la sicurezza delle informazioni sono definiti, misurati e riesaminati periodicamente nell'ambito del processo di riesame della Direzione, in coerenza con gli indicatori di performance (KPI) previsti dal Sistema di Gestione.

BREVE TERMINE (1-3 anni)

Obiettivo	Strategia
8	Sensibilizzazione in collaborazione con il Medico Competente delle buone prassi posturali.
2	Digitalizzazione dei processi Salute e Sicurezza.
2	Avviamento di un sistema di informazione tramite il Sistema Gestionale Aziendale Zucchetti
1-4-5-7-8-9	Istituzione di un sistema di funzioni e stesura delle relative procedure per la conformità alla NIS2
2 - 8	Espandere i criteri di qualifica dei fornitori anche a specifici KPI di natura ambientale e sicurezza, integrandoli nel percorso ESG.
3 - 6	Revisione completa dei progetti di prodotto con criteri di ecodesign.

MEDIO TERMINE (3-6 anni)

Obiettivo	Strategia
5	Coinvolgimento attivo dei lavoratori nella progettazione delle misure di miglioramento, conseguenti all'individuazione di criticità nel processo produttivo.
5 - 8	Premialità dei lavoratori in base ai comportamenti virtuosi in ambito ambiente e sicurezza.
1-2-4-5-7-8-9	Rafforzamento della postura di cybersicurezza dell'azienda

LUNGO TERMINE (6-9 anni)

Obiettivo	Strategia
3 - 6	Revisione completa dei progetti di prodotto con criteri di ecodesign.
1-2-4-5-7-8-9	Certificazione ISO/IEC 27001

Ogni responsabile di funzione deve rispondere, nell'ambito delle proprie competenze, del conseguimento degli obiettivi stabiliti. Ogni problema che non possa essere risolto a livello della specifica funzione dovrà essere riportato alla Direzione.

Tutto il personale è chiamato a dare il proprio contributo per l'attuazione di questa Politica, consapevole dell'importanza che essa riveste per l'affermazione dell'Azienda.

Impegno dell'Alta Direzione

L'Alta Direzione di **Concetti S.p.A.** si assume la responsabilità di attuare questa politica, diffonderla a tutti i livelli dell'organizzazione e comunicarla a tutte le parti interessate. La politica è regolarmente riesaminata per garantirne l'adeguatezza, l'efficacia e la conformità con gli obiettivi aziendali.

Bastia Umbra, 15/01/2026

Firma del Rappresentante Legale o Direzione


.....

Dott. Ing. Emanuele Concetti

REV.	NATURA DELLA REVISIONE
00	Prima emissione
01	Seconda emissione del 15.01.2026