1. Scopo

La presente Policy definisce i principi, gli indirizzi e le regole generali adottate da CORIPET per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni, sistemi informatici, reti, sistemi di automazione industriale e controllo, impianti, servizi digitali e continuità operativa della raffineria contro minacce cyber, eventi accidentali, errori umani e attacchi intenzionali.

La Policy supporta la sicurezza e la disponibilità dei processi di pianificazione, coordinamento e monitoraggio delle attività correlate al recupero/riciclo degli imballaggi in PET per liquidi alimentari e relativi semilavorati e accessori di imballaggio intercettati tramite la raccolta differenziata e selettiva con eco compattatori, al fine del raggiungimento degli obiettivi normativi di avvio al riciclo di tale tipologia di imballaggi, ma anche per il processo dello sviluppo di iniziative di promozione e di informazione dirette a sensibilizzare gli utenti finali e ad incentivare la raccolta del PET, infine, anche per tutto ciò che riguarda l'erogazione dei servizi offerti ai propri clienti e stakeholder.

2. Campo di applicazione

La Policy si applica a personale dipendente, dirigenti, operatori, collaboratori, consulenti, manutentori, fornitori e terze parti che accedono a reti, impianti, dati o locali aziendali.

Rientrano nel perimetro sedi, data center, reti, endpoint, servizi cloud, sistemi di videosorveglianza (ove presenti) e controllo accessi, backup e supporti rimovibili.

3. Riferimenti

La presente Policy è sviluppata tenendo conto, di Direttiva (UE) 2022/2555 - NIS2, normativa nazionale di settore, ISO/IEC 27001, NIST Cybersecurity Framework 2.0, Reg. UE 679/2016 (GDPR).

4. Principi generali

4.1 Approccio basato sul rischio

Le decisioni di cybersecurity e per la sicurezza delle informazioni sono assunte sulla base della valutazione dei rischi per persone, impianti, ambiente, continuità operativa, dati e obblighi normativi.

4.2 Security by design e by default

Nuovi sistemi, modifiche, integrazioni, collegamenti remoti e nuove applicazioni devono essere progettati o configurati con criteri di sicurezza adeguati fin dall'origine.

4.3 Defense in depth

La protezione deve essere multilivello e combinare misure organizzative, procedurali, fisiche e tecniche.

4.4 Minimum privilege e need-to-know

Ogni accesso deve essere concesso nella misura strettamente necessaria allo svolgimento del ruolo assegnato.

4.5 Responsabilità diffusa

La cybersecurity e la sicurezza delle informazioni è responsabilità comune della Direzione, delle funzioni tecniche, dei responsabili di processo, degli utenti e delle terze parti.

4.6 Continuità e resilienza

Le misure per la sicurezza delle informazioni e di cybersecurity devono contribuire alla resilienza dei processi critici e alla capacità di risposta e ripristino.

5. Obiettivi della cybersecurity e della sicurezza delle informazioni

- mantenere un livello adeguato di protezione dei sistemi aziendali;

- prevenire accessi non autorizzati, alterazioni, indisponibilità e dispersione di informazioni;
- ridurre probabilità e impatto di incidenti cyber su produzione, safety, ambiente e supply chain;
- rilevare tempestivamente anomalie, attacchi e compromissioni;
- assicurare pronta gestione degli incidenti e ripristino delle funzioni essenziali;
- controllare i rischi connessi a fornitori, manutentori e accessi remoti;
- promuovere formazione, consapevolezza e comportamento sicuro del personale.

6. Ruoli e responsabilità

6.1 Alta Direzione

Approva la Policy, assicura indirizzo, risorse e priorità, definisce il livello di rischio accettabile e riceve periodicamente informazioni sullo stato della sicurezza cyber.

6.2 Area IT

Coordina le azioni tra IT, engineering, operations, HSE, manutenzione, compliance e procurement; esamina rischi, incidenti, piani di trattamento e priorità di investimento.

6.3 Responsabile IT

Garantisce la sicurezza dei sistemi informativi aziendali, delle reti office e delle piattaforme digitali di competenza.

Propone regole, standard e controlli; coordina risk assessment, monitoraggio, gestione degli incidenti e miglioramento; supporta le funzioni aziendali.

6.4 Responsabili di funzione

Assicurano che il personale conosca e applichi le regole di cybersecurity e della sicurezza delle informazioni pertinenti.

6.5 Utenti

Devono utilizzare sistemi e informazioni in modo corretto, prudente e conforme alle regole aziendali, segnalando tempestivamente anomalie o incidenti.

6.6 Fornitori e terze parti

Sono tenuti a rispettare le regole contrattuali e di sicurezza applicabili, incluse quelle su accessi remoti, manutenzione, protezione dei dati, gestione vulnerabilità e notifica di eventi rilevanti.

7. Regole generali di sicurezza

7.1 Gestione degli asset

Tutti gli asset informatici devono essere identificati, censiti e classificati in funzione di criticità, proprietario, ubicazione, connessioni e dipendenze operative.

7.2 Controllo degli accessi

Gli accessi devono essere nominativi, autorizzati secondo ruolo e mansione, riesaminati periodicamente e revocati in caso di variazione o cessazione. Sono vietati, salvo eccezioni formalmente autorizzate e tracciate, account condivisi e accessi remoti non autorizzati.

7.3 Sicurezza delle credenziali

Le credenziali devono essere gestite in modo sicuro e non condivise; i dispositivi di autenticazione devono essere protetti e le credenziali compromesse sostituite immediatamente.

7.4 Segmentazione e segregazione delle reti

La rete OT (ove applicabile) deve essere segregata dalla rete IT. I flussi tra domini diversi devono essere limitati, autorizzati, documentati e monitorati; gli accessi devono avvenire tramite architetture controllate.

7.5 Gestione delle vulnerabilità e degli aggiornamenti
Le vulnerabilità devono essere analizzate in funzione del rischio effettivo. Patch e aggiornamenti devono essere pianificati, testati e approvati.

7.6 Protezione endpoint e server
Devono essere adottate misure adeguate come hardening, antimalware/EDR, controllo applicazioni, limitazione privilegi locali, protezione dei supporti rimovibili, logging e backup delle configurazioni critiche.

7.7 Backup e ripristino
Dati e configurazioni critiche devono essere oggetto di backup con verifiche periodiche di integrità e ripristinabilità; per i sistemi essenziali devono essere valutati backup offline o segregati e prove periodiche di restore.

7.8 Gestione delle modifiche
Le modifiche a sistemi, reti, applicazioni e componenti IT devono essere soggette a valutazione preventiva, autorizzazione, test, tracciabilità e riesame post-implementazione.

7.9 Accessi remoti e manutenzione da terzi
Ogni accesso remoto di fornitori e manutentori deve essere autorizzato preventivamente, limitato nel tempo e nello scopo, tracciato e consentito solo verso sistemi strettamente necessari.

7.10 Posta elettronica, navigazione web e phishing
Gli utenti devono adottare comportamenti prudenti nella gestione di email, allegati, link e file e segnalare immediatamente tentativi di phishing o social engineering.

7.11 Supporti rimovibili
L'uso di supporti USB e altri dispositivi rimovibili è consentito solo se autorizzato e controllato.

7.12 Protezione delle informazioni
Le informazioni aziendali devono essere classificate e protette in funzione della criticità, sensibilità e impatto operativo, commerciale, legale o reputazionale.

8. Monitoraggio, logging e rilevazione

L'Organizzazione adotta misure di monitoraggio e registrazione proporzionate alla criticità dei sistemi, con particolare attenzione a accessi e privilegi, firewall, sistemi di autenticazione, server, endpoint, apparati di rete, attività di manutenzione remota e tentativi di accesso falliti.

I log devono essere protetti contro alterazione e cancellazione non autorizzata e conservati secondo i criteri aziendali e normativi applicabili.

9. Gestione degli incidenti

Tutti i dipendenti, collaboratori e terze parti devono segnalare immediatamente malware, ransomware, phishing, perdita o alterazione di dati, accessi non autorizzati, compromissione di account, anomalie su reti o sistemi industriali e interruzioni sospette di servizi o apparati.

Il processo di gestione degli incidenti prevede almeno presa in carico, classificazione, contenimento, analisi tecnica, valutazione d'impatto, eradicazione, ripristino, comunicazioni interne ed esterne, raccolta delle evidenze e lesson learned.

10. Gestione dei fornitori e della supply chain

I fornitori che possono incidere sulla cybersecurity e sicurezza delle informazioni sono valutati in funzione della criticità del servizio, del livello di accesso e del rischio introdotto. Devono essere previsti requisiti contrattuali di

sicurezza, notifica di incidenti, gestione delle vulnerabilità, controllo accessi remoti e restituzione o distruzione sicura di dati e credenziali a fine rapporto.

11. Formazione e consapevolezza

Tutto il personale deve ricevere formazione e sensibilizzazione periodica sui rischi cyber e della sicurezza delle informazioni pertinenti al proprio ruolo. Devono essere previsti percorsi specialistici per personale IT, amministratori di sistema e responsabili di funzione.

12. Continuità operativa e resilienza

La cybersecurity è parte integrante della resilienza aziendale. I sistemi e i processi critici devono essere inclusi nelle attività di business continuity, disaster recovery, prove di ripristino ed esercitazioni con coordinamento tra cyber incident response, crisis management, operations e HSE.

13. Conformità, verifiche e miglioramento continuo

L'Organizzazione verifica periodicamente l'attuazione della presente Policy attraverso monitoraggi, audit, assessment tecnici, verifiche documentali ed esercitazioni. Le carenze rilevate sono gestite tramite azioni correttive, piani di trattamento e riesami periodici.

14. Violazioni della policy

La violazione della presente Policy può comportare provvedimenti disciplinari, sospensione o revoca degli accessi, escalation interne, azioni contrattuali verso fornitori e, ove dovuto, comunicazioni alle autorità competenti.

15. Approvazione, diffusione e riesame

La presente Policy è approvata dall'Alta Direzione, comunicata a tutto il personale e gli stakeholder, viene riesaminata almeno annualmente oppure a fronte di incidenti gravi, cambiamenti organizzativi, tecnologici o normativi rilevanti.

Milano, 15/04/2026

La Direzione

(Giovanni Albetti)