**11 giugno, 2025**

**ATIT_0010_ALL2**

# Politica Integrata

## Sistema di Gestione Integrato (SGI) della Sicurezza delle Informazioni, della Gestione dei Servizi e della Continuità Operativa

| | |
|---|---|
| Codice: | ATIT_0010_ALL2 |
| Revisione: | 07 |
| Data di revisione: | 03/08/2026 |
| Redatta da: | Enrico Minelle |
| Approvata da: | Andrea Moschetti |
| Livello di riservatezza: | Public |

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

## Tabella delle revisioni

| Data | Oggetto | Autore | Versione | Status | Class. |
|---|---|---|---|---|---|
| 29.05.2025 | Inizio redazione preliminare | Enrico Minelle | 01 | WIP | **MGTR** |
| 30.05.2025 | Documento predisposto per la lettura draft | Enrico Minelle | 02 | DRA | **MGTR** |
| 09.06.2025 | Revisione lessicale e correzioni | Luca Bauckneht | 03 | DRA | **MGTR** |
| 28.08.2025 | Pubblicazione | Enrico Minelle | 04 | REL | **PUBL** |
| 26.09.2025 | Meglio specificata aderenza ISO27017/18. | Enrico Minelle | 05 | DRA | **PUBL** |
| 10.07.2026 | Integrazione ISO 22301 e ISO 20000 | Laura Pietrosemoli | 06 | WIP | **PUBL** |
| 03.08.2026 | Revisione e Pubblicazione | Enrico Minelle | 07 | REL | **PUBL** |

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

## Indice


1. Premessa ..... 4
2. Scopo ed Obiettivi ..... 4
3. Campo di Applicazione ..... 4
4. Politica della Sicurezza delle Informazioni ..... 5
5. Sicurezza delle informazioni nei servizi cloud e protezione dei dati personali ..... 7
6. Politica per la gestione dei servizi ..... 7
7. Politica per la continuità operativa ..... 8
8. Responsabilità di Osservanza e di Attuazione ..... 8
9. Riesame ..... 9
10. Impegno della direzione ..... 10

A. APPENDICE UNO: Classificazione dei Documenti e Legenda ..... 12


Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

## 1. PREMESSA

La sicurezza delle informazioni, l'affidabilità dei servizi e la capacità di assicurare la continuità delle attività rappresentano valori fondamentali per **FAAC Technologies** e costituiscono parte integrante della cultura, della governance e dei processi aziendali.

In un contesto economico e tecnologico in continua evoluzione, caratterizzato da minacce informatiche crescenti e da obblighi normativi sempre più stringenti, la protezione del patrimonio informativo rappresenta un presupposto essenziale per garantire la fiducia dei clienti, dei partner e delle parti interessate, oltre che per preservare la reputazione e la competitività dell'azienda.

La presente Politica si inserisce in tale quadro come espressione dell'impegno della Direzione a mantenere elevati standard di integrità, responsabilità e consapevolezza nella gestione delle informazioni, fornendo il riferimento strategico su cui si fonda il Sistema di Gestione Integrato (SGI), sviluppato in coerenza con le norme ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 20000-1 e ISO 22301, nelle versioni applicabili, nonché con i requisiti legislativi, regolamentari e contrattuali pertinenti.

## 2. SCOPO ED OBIETTIVI

Lo scopo della presente Politica è garantire che tutte le informazioni trattate da **FAAC Technologies** siano protette da minacce, vulnerabilità e rischi che possano comprometterne riservatezza, integrità, disponibilità o conformità normativa.

La Politica ha i seguenti obiettivi fondamentali:

- **Proteggere il patrimonio informativo aziendale**, assicurando che i dati siano accessibili solo a persone autorizzate, completi e accurati, disponibili quando necessario.
- **Supportare la continuità operativa** e la qualità dei servizi offerti a clienti e partner, anche in presenza di eventi imprevisti.
- **Garantire la conformità a norme, regolamenti e obblighi contrattuali**, incluse le disposizioni del GDPR e degli standard internazionali ISO/IEC 27001:2022, ISO/IEC 27017:2021, ISO/IEC 27018:2020, ISO/IEC 20000-1:2018 e ISO 22301:2019
- **Promuovere la consapevolezza e la responsabilità del personale**, favorendo comportamenti sicuri e coerenti con i principi aziendali.
- **Pianificare, progettare, realizzare, mettere in esercizio, erogare, monitorare e migliorare servizi affidabili**, sicuri e coerenti con i requisiti concordati.
- **Prevenire e ridurre la probabilità e l'impatto di interruzioni**, assicurando una risposta coordinata e il ripristino delle attività e dei servizi entro livelli e tempi accettabili.
- **Sostenere il miglioramento continuo** del Sistema di Gestione Integrato (SGI), attraverso attività di analisi, monitoraggio, audit e riesame periodici.

Attraverso questi obiettivi, **FAAC Technologies** si impegna a rendere la sicurezza delle informazioni un fattore abilitante per il business, la fiducia delle parti interessate e la reputazione aziendale

## 3. CAMPO DI APPLICAZIONE

La presente politica si applica nell'ambito della:

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

PROGETTAZIONE, SVILUPPO E MANUTENZIONE DI PIATTAFORME DIGITALI, APPLICAZIONI SOFTWARE E COMPONENTI HARDWARE PER SISTEMI DI AUTOMAZIONE, ACCESSI PEDONALI E VEICOLARI CON O SENZA ESAZIONE DELLA SOSTA, GESTITI PRESSO LA CAPOGRUPPO, COMPRESI I PROCESSI DI RICERCA E SVILUPPO, INFORMATION TECHNOLOGY, ESERCIZIO E MANUTENZIONE DI SERVIZI INTEGRATI PER LA GESTIONE E IL MONITORAGGIO DEI DISPOSITIVI, PRODUZIONE E SUPPORTO CLIENTI.

Il perimetro sopra definito costituisce il campo di applicazione unico del Sistema di Gestione Integrato e si applica in maniera coincidente a tutte le norme adottate. In particolare, il medesimo ambito organizzativo, tecnologico e di servizio si intende valido per:

- **ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2020**, con riferimento alla sicurezza delle informazioni, alla sicurezza dei servizi cloud e alla protezione dei dati personali trattati in cloud;
- **ISO/IEC 20000-1:2018**, con riferimento alla progettazione, erogazione, supporto e miglioramento dei servizi ricompresi nel perimetro;
- **ISO 22301:2019**, con riferimento alla continuità operativa delle attività, dei prodotti e dei servizi prioritari individuati all'interno del medesimo ambito.

L'organizzazione dichiara pertanto che non sussistono perimetri differenziati tra le norme del Sistema di Gestione Integrato: le attività, le sedi, i processi, i servizi e le risorse ricompresi nel campo di applicazione sono i medesimi per tutti gli standard adottati, garantendo un presidio coerente e unitario dei requisiti di sicurezza delle informazioni, gestione dei servizi e continuità operativa.

La Politica è vincolante per tutto il personale e si applica, per quanto pertinente, ai collaboratori, ai fornitori, ai partner e a ogni soggetto esterno che possa accedere a informazioni, asset, processi o servizi compresi nel perimetro del Sistema di Gestione Integrato.

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

## 4. Politica della Sicurezza delle Informazioni

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.

È necessario assicurare:

- la confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da chi ha un interesse precipuo nella consultazione/utilizzo delle stesse ed è formalmente autorizzato ad accedervi;
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione;
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare:

- il danneggiamento dell'immagine e della reputazione aziendale;
- la mancata soddisfazione del cliente;

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

- il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti;
- danni di natura economica e finanziaria.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo.

La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno di essi deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali, nonché di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

## 5. SICUREZZA DELLE INFORMAZIONI NEI SERVIZI CLOUD E PROTEZIONE DEI DATI PERSONALI

FAAC Technologies riconosce che l'utilizzo di servizi di cloud computing rappresenta un fattore abilitante per l'innovazione e l'efficienza, ma comporta anche rischi specifici che devono essere gestiti con la massima attenzione.

In coerenza con gli standard internazionali **ISO/IEC 27017** e **ISO/IEC 27018**, l'organizzazione si impegna a garantire che la sicurezza delle informazioni e la protezione dei dati personali siano sempre tutelate anche quando i trattamenti avvengono in ambienti cloud.

A tal fine la Direzione assicura che:

- **Tutela delle informazioni**
  Tutti i dati gestiti nei servizi cloud sono protetti da accessi non autorizzati, da perdita o da alterazioni, e sono trattati in conformità con i livelli di rischio accettabili definiti dal SGSI.
- **Affidabilità dei fornitori cloud**
  I fornitori di servizi cloud devono adottare misure tecniche e organizzative adeguate, che includano la separazione logica degli ambienti multi-tenant, controlli sugli amministratori privilegiati, tracciabilità delle attività e procedure di cancellazione sicura dei dati al termine del servizio.
- **Localizzazione e trasferimenti dei dati**
  L'organizzazione mantiene consapevolezza e controllo sulla localizzazione geografica dei dati, richiedendo che eventuali trasferimenti internazionali avvengano nel rispetto delle leggi applicabili e siano sempre autorizzati e tracciabili.
- **Protezione dei dati personali**
  I dati personali trattati in cloud sono gestiti nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione. Il trattamento avviene esclusivamente sulla base di istruzioni documentate, con particolare attenzione a consenso, diritti degli interessati e conformità al GDPR.
- **Responsabilità condivisa**
  L'utilizzo dei servizi cloud si fonda su una chiara definizione delle responsabilità tra FAAC Technologies, i fornitori e gli utenti interni, affinché ciascun attore contribuisca alla sicurezza complessiva delle informazioni e alla protezione dei dati personali.

La Direzione riafferma con questa politica il proprio impegno a un utilizzo sicuro, conforme e responsabile dei servizi cloud, rafforzando la fiducia delle parti interessate, sostenendo la resilienza aziendale e garantendo la protezione dei diritti fondamentali delle persone

## 6. POLITICA PER LA GESTIONE DEI SERVIZI

In coerenza con lo standard ISO/IEC 20000-1:2018, **FAAC Technologies** si impegna a stabilire, attuare, mantenere e migliorare continuamente un Sistema di Gestione dei Servizi (integrato in SGI) in grado di assicurare che i servizi siano pianificati, progettati, realizzati, messi in esercizio, erogati, supportati e migliorati in modo controllato, coerente e orientato al valore.

La gestione dei servizi è indirizzata ai seguenti obiettivi:

- **mantenere un portafoglio e un catalogo dei servizi** coerenti con il perimetro, le responsabilità e gli impegni assunti;
- **definire, monitorare e riesaminare livelli di servizio e indicatori**, inclusi SLA, OLA e altri accordi di supporto pertinenti;

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

- **assicurare che progettazione, costruzione, transizione, rilascio e messa in esercizio di servizi nuovi o modificati** siano pianificati e controllati;
- **gestire in modo efficace** richieste di servizio, incidenti, problemi, modifiche, configurazioni.
- **integrare** la sicurezza delle informazioni e la protezione dei dati personali nei processi di gestione dei servizi;
- **gestire relazioni con clienti, utenti, fornitori e partner**, assicurando responsabilità e prestazioni lungo la catena di fornitura;
- **raccogliere, analizzare e utilizzare dati di performance**, feedback, reclami, non conformità e opportunità di miglioramento;

I servizi devono essere erogati secondo processi chiari, documentati, ripetibili e proporzionati alla loro criticità. Eventuali scostamenti dai requisiti concordati devono essere rilevati, comunicati, gestiti e analizzati per prevenire il ripetersi delle cause. La gestione dei servizi è attuata in modo integrato con la sicurezza delle informazioni e la continuità operativa, assicurando il rispetto dei requisiti applicabili della norma ISO/IEC 20000-1:2018 lungo l'intero ciclo di vita dei servizi.

## 7. Politica per la continuità operativa

In coerenza con lo standard ISO 22301:2019, **FAAC Technologies** si impegna a sviluppare e mantenere una capacità organizzativa di prevenzione, preparazione, risposta e ripristino rispetto a eventi che possano interrompere processi, risorse, sedi, tecnologie, forniture o servizi critici.
Il Sistema di Gestione per la Continuità Operativa (integrato in SGI) è finalizzato a:

- **identificare attività, prodotti e servizi prioritari** mediante analisi di impatto sul business (BIA) e valutazione dei rischi di interruzione;
- **stabilire obiettivi di ripristino, priorità, tempi,** capacità minima accettabile e requisiti di recupero dei dati per i processi e i servizi pertinenti;
- **predisporre, mantenere e rendere disponibili piani e procedure di risposta**, gestione della crisi, comunicazione e ripristino;
- **coordinare la continuità operativa** con la gestione degli incidenti di sicurezza, degli incidenti di servizio e delle emergenze;
- **condurre esercitazioni, simulazioni e test periodici**, valutandone i risultati e attuando le azioni di miglioramento necessarie;
- **ridurre gli impatti economici, operativi, legali, reputazionali** e sulle persone derivanti da eventi interruttivi.

Il Sistema di Gestione per la Continuità Operativa è attuato in modo integrato con la sicurezza delle informazioni e la gestione dei servizi, assicurando il rispetto dei requisiti applicabili della norma ISO 22301:2019 e la salvaguardia delle attività e dei servizi prioritari individuati all'interno del perimetro.

## 8. Responsabilità di Osservanza e di Attuazione

L'osservanza e l'attuazione delle politiche sono responsabilità di:

1. Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
   Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
2. Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente politica.

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Il Responsabile del Sistema di Gestione integrato, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- **condurre l'analisi dei rischi** con le opportune metodologie e adottare tutte le misure per la gestione del rischio
- **stabilire tutte le norme necessarie** alla conduzione sicura di tutte le attività aziendali
- **verificare le violazioni** alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
- **organizzare la formazione** e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
- **verificare periodicamente l'efficacia** e l'efficienza del Sistema di Gestione.

Chiunque, - dipendenti, consulenti e/o collaboratori esterni dell'Azienda -, disattenda le regole di sicurezza stabilite, in modo intenzionale o riconducibile a negligenza, provocando in tal modo un danno all'azienda, anche meramente potenziale, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

## 9. RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione Integrato, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della politica in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

Il Responsabile del Sistema di Gestione Integrato ha la responsabilità del riesame della politica.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive, nonché l'aderenza alla politica.

Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio dell'azienda alla gestione della sicurezza delle informazioni, dei servizi e della continuità operativa, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e i risultati dei precedenti riesami.

In coerenza con i requisiti applicabili delle norme adottate, il riesame prende in considerazione, tra gli altri, i seguenti elementi in ingresso:

- **gli esiti delle valutazioni del rischio** e lo stato del trattamento dei rischi per la sicurezza delle informazioni;
- **le prestazioni dei servizi** rispetto ai livelli concordati, inclusi il rispetto degli SLA e degli OLA, i reclami e la soddisfazione degli utenti e dei clienti;
- **gli esiti delle analisi di impatto** sul business (BIA) e delle esercitazioni, simulazioni e test di continuità operativa, unitamente allo stato di aggiornamento dei relativi piani;
- **gli incidenti** di sicurezza, gli incidenti di servizio e gli eventi interruttivi occorsi, con le relative azioni intraprese;
- **l'esito degli audit interni ed esterni**, delle non conformità e delle azioni correttive;
- **il grado di conseguimento degli obiettivi** del Sistema di Gestione Integrato e dei relativi indicatori di prestazione.

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni, dei servizi e della continuità operativa, nonché eventuali esigenze di modifica del Sistema di Gestione Integrato, della presente politica e delle risorse necessarie

## 10. Impegno della Direzione

La Direzione sostiene attivamente la sicurezza delle informazioni, la gestione dei servizi e la continuità operativa in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative al Sistema di Gestione Integrato.

L'impegno della Direzione si attua tramite una struttura i cui compiti sono:

- **garantire** che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni, alla gestione dei servizi e alla continuità operativa e che questi incontrino i requisiti aziendali;
- **stabilire** i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione Integrato;
- **fornire risorse** sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione Integrato;
- **controllare** che il Sistema di Gestione Integrato sia adottato in tutti i processi aziendali, in modo che procedure e controlli siano sviluppati efficacemente;
- **assicurare** che il Sistema di Gestione Integrato consegua i risultati attesi in termini di protezione delle informazioni, erogazione di servizi conformi ai livelli concordati e capacità di garantire la continuità delle attività e dei servizi prioritari;
- **approvare e sostenere** tutte le iniziative volte al miglioramento della sicurezza delle informazioni, della qualità dei servizi e della resilienza operativa;
- **attivare programmi** per la diffusione della consapevolezza e della cultura in materia di sicurezza delle informazioni, gestione dei servizi e continuità operativa.

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

La presente Politica entra in vigore dalla data della sua approvazione ed è vincolante per tutto il personale dell'organizzazione, nonché per i collaboratori e fornitori che trattano informazioni, erogano o supportano servizi rientranti nel perimetro del Sistema di Gestione Integrato.

La Direzione garantisce che la Politica sia riesaminata almeno una volta all'anno, o comunque ogniqualvolta intervengano modifiche significative nel contesto organizzativo, tecnologico o normativo.

Con l'apposizione della firma, la Direzione approva formalmente la presente Politica e ne sancisce la diffusione interna ed esterna secondo le modalità previste dal Sistema di Gestione Integrato.

Zola Predosa, lì 03/08/2026

Il Presidente Esecutivo: Andrea Moschetti

Firma: 

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

# A. APPENDICE UNO: CLASSIFICAZIONE DEI DOCUMENTI E LEGENDA

Legenda per il titolo del documento:

**CPxx_yyyy_zz_title**: **Corporate Policy**, lingua, numero fascicolo, revisione, titolo
**CDxx_yyyy_zz_title**: **Corporate Document**, lingua, numero fascicolo, revisione, titolo
**MNxx_yyyy_zz_title:** **Manual,** lingua, numero fascicolo, revisione, titolo
**GP_kkk_yyyy_zz_title:** **Global Procedure**, area funzionale, numero fascicolo, revisione, titolo
**LP_kkk_yyyy_zz_title:** **Local Procedure**, area funzionale, numero fascicolo, revisione, titolo
**MD_yyyy_zz_title:** **Module,** numero fascicolo, revisione, titolo
**ATxx_yyyy_zz_title:** **Attachment,** lingua, numero fascicolo, revisione, titolo

Legenda per lo stato della redazione del documento:

**WIP**: Work in Progress. Non rilasciato.
**DRA**: Draft. Rilasciato a specifiche persone per correzioni.
**PRE**: Preliminary. Rilasciato per lettura. Possono ancora essere aggiunti commenti minori.
**REL**: Released. Rilasciato
**OBS**: Obsolete. Tolto dalla disponibilità.

Legenda per la classificazione del documento:

**PUBL:** **Public**. Documenti destinati al consumo pubblico, la cui diffusione non comporta rischi per il Gruppo FAAC anche qualora finissero in luoghi non appropriati. In genere si assume inoltre che un documento privo di etichetta sia considerato pubblico.
**NDAC:** **NDA Confidential**. Documenti che devono essere visionati esclusivamente da destinatari vincolati da un accordo di riservatezza (NDA).
**EMPC:** **Employee Confidential**. Documenti che devono essere visionati esclusivamente da destinatari che siano dipendenti (a tempo pieno o parziale).
**MGTR:** **Management Restricted**. Documenti che devono essere visionati esclusivamente dal senior management del Gruppo FAAC e non dall'intera comunità dei dipendenti.
**EXEC:** **Executives Restricted**. Documenti che devono essere visionati esclusivamente dai primi livelli di governo del Gruppo FAAC (Direzione Generale e top executives), ma non dall'intera comunità manageriale
**BRDR:** **Board Restricted**. Documenti che devono essere visionati esclusivamente dal Consiglio di Amministrazione.
**PRIV:** **Private.** Documenti contenenti informazioni personali identificative, tipicamente relative a dati sanitari, finanziari o ad altre informazioni di carattere personale.

Dipendenti di Information Technology che firmano clausole di confidenzialità all'interno dei loro contratti raggiungono il livello di **MGTR** nella sola documentazione relativa all'Information Technology.

Il presente documento è di proprietà di FAAC S.p.A. e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.