CAA FAPI

PROTEGGIAMO DATI E DOCUMENTI

Regole di sicurezza per le sedi operative

ACCESSO ALLE AREE RISERVATE: SOLO PERSONALE AUTORIZZATO

Tuteliamo le informazioni da accessi indebiti, divulgazione, perdita e alterazione.

Le regole riguardano locali, archivi, documenti, sistemi e cartelle digitali individuati come riservati e si applicano a dipendenti, collaboratori e soggetti autorizzati.

LE REGOLE DA RISPETTARE OGNI GIORNO

- **ACCESSI LIMITATI.** Accedi solo alle aree e alle informazioni autorizzate e necessarie alle tue mansioni.
- **LOCALI E ARCHIVI CHIUSI.** Chiudi porte e armadi riservati quando non utilizzati o presidiati. Custodisci chiavi e badge: non cederli a persone non autorizzate.
- **VISITATORI ACCOMPAGNATI.** L'accesso alle aree riservate richiede preventiva autorizzazione e accompagnamento secondo la procedura interna. Non consentire consultazioni estranee all'attività autorizzata.
- **DOCUMENTI AL SICURO.** Non lasciare documenti e supporti incustoditi o visibili a persone non autorizzate. Al termine dell'attività riponili negli spazi previsti.
- **CREDENZIALI PERSONALI.** Non condividere le credenziali. Blocca la postazione quando ti allontani e utilizza soltanto strumenti e modalità di accesso autorizzati.
- **INVII E COPIE CONTROLLATI.** Copia, esporta o trasmetti informazioni solo per esigenze di servizio, verificando i destinatari e usando canali autorizzati. Non utilizzare account personali o dispositivi e supporti non autorizzati.
- **CONSERVAZIONE E SMALTIMENTO SICURI.** Rispetta i tempi di conservazione previsti. Elimina documenti e supporti soltanto con modalità autorizzate che impediscano recuperi o consultazioni indebite.

NOTI UN'ANOMALIA? SEGNALALA SUBITO

Accessi sospetti, chiavi o badge smarriti, documenti o dispositivi persi, invii errati: avvisa tempestivamente il referente indicato sotto. Segui le istruzioni ricevute, senza iniziative non autorizzate.

LA SICUREZZA DELLE INFORMAZIONI È UN IMPEGNO QUOTIDIANO

Prendi visione della policy e rispetta le disposizioni applicabili.

CAA FAPI S.R.L.
Policy per la protezione delle aree riservate, dei dati e dei documenti

Approvata da: CdA CAA FAPI S.r.l. · **Data di approvazione:** 30/03/2025
Referente della policy: Dott. Giuseppe Mastrandrea Direttore Tecnico CAA FAPI

1. Finalità e ambito di applicazione
La presente policy disciplina la protezione delle aree fisiche e degli ambienti digitali riservati delle sedi operative del CAA FAPI, al fine di tutelare la riservatezza, l'integrità e la disponibilità delle informazioni. Si applica a dipendenti, collaboratori e altri soggetti autorizzati che accedono a locali, archivi, documenti, sistemi o cartelle digitali nell'ambito delle attività del Centro di Assistenza Agricola. Le disposizioni relative ai visitatori e ai fornitori devono essere comunicate prima dell'accesso alle aree interessate.

2. Informazioni critiche e individuazione delle aree riservate
Sono considerate critiche le informazioni la cui divulgazione, alterazione, perdita o indisponibilità potrebbe compromettere la tutela degli interessati, la sicurezza o la continuità delle attività. Rientrano in tale ambito, ove trattati dalla sede, fascicoli e pratiche delle aziende agricole, mandati, documenti identificativi, documentazione aziendale e amministrativa, dati economici e coordinate bancarie, credenziali e documenti interni riservati. Il responsabile di sede mantiene un elenco aggiornato dei locali, degli armadi, degli archivi e degli ambienti digitali da proteggere, indicando i soggetti autorizzati e le modalità di custodia. L'elenco e le informazioni sui sistemi di accesso non devono essere esposti al pubblico.

3. Ruoli e responsabilità
- **Direzione o funzione competente:** approva la policy, individua i referenti e assicura il coordinamento delle misure organizzative.
- **Responsabile di sede:** individua le aree riservate, propone le autorizzazioni, cura la custodia di chiavi e badge, diffonde le istruzioni e verifica l'applicazione delle regole.
- **Referente informatico incaricato:** gestisce gli accessi digitali e le misure tecniche di competenza, secondo le autorizzazioni ricevute e le procedure applicabili.
- **Personale autorizzato:** utilizza le informazioni nei limiti delle mansioni, osserva le istruzioni e segnala tempestivamente anomalie e incidenti.
- **Referente per le anomalie:** riceve le segnalazioni e attiva le funzioni competenti. Nominativi, incarichi e recapiti devono essere formalizzati e comunicati al personale.

4. Autorizzazioni e accessi fisici
L'accesso alle aree riservate è consentito soltanto previa autorizzazione della funzione competente e nei limiti necessari alle mansioni. Le autorizzazioni devono essere documentate, riesaminate in caso di variazione dell'incarico e revocate alla cessazione delle esigenze di accesso. La consegna e la restituzione di chiavi e badge devono essere registrate; è vietata la loro cessione a persone non autorizzate. Porte, armadi e archivi riservati devono essere mantenuti chiusi quando non utilizzati o presidiati. Il responsabile di sede definisce le verifiche di chiusura al termine della giornata e il soggetto incaricato di effettuarle.

5. Visitatori, utenti e fornitori
Utenti e visitatori devono essere ricevuti negli spazi destinati all'accoglienza, evitando l'esposizione di pratiche o informazioni riferite ad altri soggetti. L'accesso di persone esterne alle aree riservate richiede preventiva autorizzazione e accompagnamento secondo la procedura della sede. Gli interventi di manutenzione devono essere organizzati in modo da limitare l'accesso alle informazioni alle sole esigenze dell'intervento. Eventuali registrazioni degli accessi devono contenere soltanto le informazioni necessarie ed essere custodite secondo le procedure applicabili.

6. Custodia e movimentazione dei documenti
Fascicoli, stampe e supporti non devono essere lasciati incustoditi sulle scrivanie, presso stampanti o in luoghi accessibili a persone non autorizzate. Al termine dell'attività devono essere riposti negli spazi previsti. Durante colloqui e consultazioni occorre impedire la visione di documenti e schermate estranei alla pratica trattata. Il prelievo, il trasferimento tra sedi e l'eventuale utilizzo fuori sede devono essere autorizzati e tracciati con modalità proporzionate, assicurando custodia e riconsegna. Non è consentito fotografare, riprodurre o asportare documenti per finalità estranee al servizio.

7. Credenziali e ambienti digitali
Le credenziali sono personali e non devono essere condivise o rese accessibili ad altri. È vietato utilizzare l'account di un altro operatore. Le postazioni devono essere bloccate ogni volta che ci si allontana. Documenti e dati devono essere salvati esclusivamente negli ambienti autorizzati, con permessi coerenti con le mansioni. Non devono essere utilizzati account personali, servizi cloud, software, dispositivi o supporti non autorizzati. Il referente informatico definisce e documenta, per i sistemi di competenza, le misure di autenticazione, aggiornamento, protezione, copia di sicurezza e ripristino, verificandone l'effettiva applicazione; per i sistemi esterni si osservano anche le istruzioni del relativo gestore.

8. Copie, esportazioni e trasmissioni
Copie, esportazioni e invii sono consentiti esclusivamente per esigenze di servizio e nei limiti dell'autorizzazione ricevuta. Prima della trasmissione, l'operatore verifica destinatario, recapito, allegati e pertinenza delle informazioni, utilizzando i canali approvati. L'eventuale protezione degli allegati deve seguire le istruzioni interne; le credenziali di apertura non devono essere comunicate insieme al documento attraverso il medesimo canale. Le richieste di consegna o comunicazione di documenti devono essere gestite previa verifica dell'identità e del titolo del richiedente, secondo le procedure applicabili.

9. Conservazione e dismissione
Il personale rispetta i tempi di conservazione stabiliti per ciascuna categoria documentale dalle procedure interne e dagli obblighi applicabili. La presente policy non introduce un termine unico di conservazione. Eliminazioni e dismissioni richiedono l'autorizzazione della funzione competente, previa verifica di eventuali esigenze di conservazione ancora sussistenti. I documenti cartacei devono essere distrutti con modalità che impediscano la ricostruzione delle informazioni; i supporti digitali devono essere affidati al referente incaricato per la cancellazione sicura o la dismissione controllata. Le copie non più necessarie seguono le medesime regole di tutela.

10. Segnalazione e gestione delle anomalie
Accessi sospetti, smarrimenti di chiavi o badge, perdita di documenti o dispositivi, invii a destinatari errati e altre possibili compromissioni devono essere segnalati senza ritardo a [referente – telefono – e-mail/canale], con eventuale contatto alternativo [recapito]. La segnalazione riporta, per quanto noto, momento della rilevazione, natura dell'evento, sede o sistema interessato e informazioni potenzialmente coinvolte, senza diffondere inutilmente dati riservati. L'operatore conserva le evidenze disponibili e si attiene alle istruzioni ricevute, evitando cancellazioni, modifiche o iniziative non autorizzate. Il referente registra l'evento e coinvolge tempestivamente le funzioni competenti per contenimento, valutazione, ripristino e verifica degli eventuali adempimenti. Le comunicazioni esterne sono riservate ai soggetti incaricati.

11. Diffusione, verifiche e aggiornamento
La policy deve essere comunicata al personale interessato, resa consultabile attraverso [ufficio/percorso interno] e accompagnata dalle istruzioni necessarie all'applicazione. La presa visione deve essere documentata. Il manifesto esposto nelle sedi costituisce un richiamo sintetico e non sostituisce la policy né le procedure operative. Il responsabile di sede verifica periodicamente autorizzazioni, custodia dei documenti, chiusura degli archivi e conoscenza dei recapiti di segnalazione; il referente informatico verifica le misure di propria competenza. Frequenza e modalità dei controlli sono definite in [piano/procedura]. Gli esiti e le azioni correttive sono documentati. La policy è riesaminata in caso di cambiamenti organizzativi, modifiche dei sistemi, incidenti significativi e secondo la scadenza [data/periodicità].