

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

Sommario

Premessa	2
Ambito	2
Gestione del rischio	3
Principi di sicurezza delle informazioni	3
Ruolo della Direzione	4
Ruolo del Responsabile della Sicurezza delle Informazioni	5
Ruolo del Personale	5
Approvazione e riesame	6

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

Premessa

La presente **Politica di Gestione della Sicurezza delle Informazioni** definisce l'insieme dei principi, degli indirizzi e degli impegni attraverso cui il CREA tutela il proprio patrimonio informativo e garantisce la continuità dei servizi istituzionali, in coerenza con la propria missione e con gli obblighi stabiliti dalla **Direttiva (UE) NIS2** e relativo recepimento nazionale.

Il CREA assume come riferimento le migliori pratiche riconosciute a livello nazionale **AGID/ACN/NIS** e internazionale, tra cui gli standard **ISO/IEC 27001**, pur non adottando formalmente un sistema di gestione certificato.

La Direzione approva la presente politica, ne assicura la diffusione a tutto il personale e ai soggetti esterni coinvolti, e si impegna a garantirne l'applicazione uniforme in tutte le strutture del CREA.

Ambito

La presente politica si applica indistintamente a tutti gli organi e livelli del CREA, è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto nel trattamento di informazioni che rientrano nel campo di applicazione del **Sistema di Gestione della Sicurezza delle Informazioni** e in coerenza con la normativa vigente e con gli obblighi NIS.

Il CREA consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività dell'ente; tali comunicazioni devono avvenire nel rispetto delle regole e delle norme cogenti.

Il patrimonio informativo del CREA comprende dati, documenti, sistemi informatici, infrastrutture tecnologiche e servizi essenziali necessari allo svolgimento delle funzioni istituzionali.

La loro protezione deve garantire:

Confidenzialità – accesso consentito esclusivamente a soggetti autorizzati;

Integrità – correttezza, completezza e affidabilità delle informazioni e dei processi;

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

Disponibilità – fruibilità dei dati e dei servizi da parte degli incaricati autorizzati nei tempi necessari.

Il mancato rispetto di adeguate misure di sicurezza può compromettere la continuità dei servizi essenziali, produrre disservizi ai cittadini e comportare obblighi di notifica, responsabilità amministrative e sanzioni, oltre a possibili danni reputazionali per il CREA.

Gestione del rischio

Il CREA adotta un approccio sistematico alla gestione del rischio, mediante attività periodiche di analisi che consentono di valutare l'esposizione a minacce interne ed esterne, identificare vulnerabilità e determinare le misure più adeguate per garantire livelli di sicurezza proporzionati alla criticità dei servizi.

I risultati dell'analisi del rischio costituiscono il fondamento per l'adozione delle misure di sicurezza tecniche, organizzative e procedurali.

Principi di sicurezza delle informazioni

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno 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;

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

- 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;
- Tutti devono notificare qualsiasi problema relativo alla sicurezza per poter gestire in modo tempestivo gli incidenti. 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'ente di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione dell'intero ente;
- Devono essere inclusi nella progettazione gli aspetti di sicurezza in tutte le fasi di 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 e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Ruolo della Direzione

La **Direzione** sostiene attivamente la sicurezza delle informazioni mediante:

- definizione degli obiettivi strategici di sicurezza in coerenza con la missione del CREA;
- assegnazione chiara di ruoli e responsabilità;
- messa a disposizione delle risorse necessarie;
- integrazione della sicurezza nei processi del CREA;
- promozione della cultura della sicurezza a tutti i livelli;
- riesame periodico della presente politica e del sistema di sicurezza, specialmente a fronte di cambiamenti significativi.

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

Ruolo del Responsabile della Sicurezza delle Informazioni

Il **Responsabile della Sicurezza delle Informazioni** si adopera per:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- definire e aggiornare le procedure e i controlli di sicurezza;
- verificare incidenti e non conformità e proporre contromisure;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
- controllare periodicamente l'efficacia delle misure adottate e proporre miglioramenti.

Ruolo del Personale

Tutto il **personale del CREA** è tenuto a operare nel rispetto delle disposizioni contenute nella presente politica e nelle procedure interne, segnalando tempestivamente eventuali anomalie o violazioni.

I soggetti esterni che collaborano con il CREA sono tenuti a rispettare i requisiti di sicurezza stabiliti nei contratti e negli accordi di servizio.

La violazione delle norme di sicurezza, se dovuta a dolo o negligenza, può comportare responsabilità disciplinari, amministrative, civili o penali, secondo quanto previsto dall'ordinamento vigente.

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

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

	SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI INFORMATION SECURITY POLICY	PSI
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 00 del 21/04/2026

Chiunque, dipendenti, consulenti e/o collaboratori esterni al CREA, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'ente, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

Approvazione e riesame

La presente politica è approvata dalla Direzione del CREA e viene riesaminata con cadenza periodica annuale o in occasione di mutamenti rilevanti nell'organizzazione, nei servizi erogati, nella normativa di riferimento o nel contesto di rischio in un'ottica di **impegno al miglioramento continuo**.