

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

# DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

## EMISSIONE DEL DOCUMENTO

### Autori

Riferimento	Nome
Uff. Sistemi Informativi	Fabio Palpini, Luca Erba, Mauro Magini, Nicola Simone, Rosella Brandini
DPO	Valentina Longo
DG	Maria Chiara Zaganelli

### Revisioni

Versione	Data	Descrizione	Nome
0.1-0.4	21/03/2026	Approvato	Luca Erba, Valentina Longo
0.5-0.6	27/03/2026	Approvato	Luca Erba, Valentina Longo
0.7	10/04/2026	Approvato	Luca Erba, Valentina Longo
1.0	21/04/2026	Approvato	Luca Erba, Valentina Longo
1.1	02/07/2026	Approvato	Luca Erba

### Registro delle Revisioni

Versione	Modifiche apportate
1.0-0.4	Predisposizione bozza e continui aggiornamenti ed integrazioni
0.5-0.6	Condivisione e razionalizzazione dei contenuti
0.7	Revisione di editing finale
1.0	Release
1.1	Integrazione con i riferimenti della delibera di approvazione da parte del CDA e della comunicazione a mezzo mail ai dipendenti

### Allegati

Identificativo	Nome Documento	Scopo
Allegato (1)	<i>Elenco software</i>	
Allegato (2)	<i>Nomina del fiduciario</i>	

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

## Sommario

Introduzione .....	4
Finalità del documento .....	4
Contesto normativo .....	5
Titolarità delle risorse informatiche .....	6
Glossario e definizioni.....	6
Principi Generali .....	7
Regole per l'utilizzo dei sistemi informativi .....	9
Credenziali di accesso .....	9
Utilizzo di applicazioni aziendali .....	10
Accesso da paesi esteri.....	11
Postazione di lavoro .....	11
Software a corredo .....	13
Navigazione internet.....	13
Stampanti.....	14
Posta elettronica.....	15
Accesso alla casella di posta per assenza del titolare dell'account.....	16
Metadati nei sistemi di posta elettronica.....	17
PEC.....	18
Disattivazione caselle di posta .....	18
Servizi di comunicazione.....	19
Servizi cloud e spazi di condivisione .....	19
Dispositivi di memorizzazione portatili.....	19
Strumenti di firma digitale .....	20
Gestione degli incidenti di sicurezza informatica .....	20
Controlli e monitoraggi .....	21
Responsabilità e sanzioni.....	22

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

## Introduzione

Il presente disciplinare (approvato nella seduta del CDA del 28-05-2026 con delibera n. 70/2026) sostituisce integralmente i precedenti adottati:

- Determina del Direttore Generale n.19 del 23.02.2011, Allegato 1;
- Determina del Direttore Generale del 13 marzo 2024 avente prot. n. 0021860 del 13/03/2024, successivamente abrogata con nota del Presidente prot. n. 0036833 del 29/04/2024.

Il CREA, nell'espletamento delle proprie attività istituzionali, opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche e operative, finalizzate sia alla prevenzione di utilizzi impropri delle strumentazioni informatiche, sia alla protezione delle informazioni trattate e conservate nelle proprie banche dati.

Il presente disciplinare definisce le regole e le condizioni di utilizzo degli strumenti informatici da parte di tutti i soggetti che, a qualsiasi titolo, intrattengono un rapporto con il CREA (dipendenti, collaboratori, consulenti, stagisti, fornitori, ecc.) e che, nell'ambito di tale rapporto, utilizzano i suddetti strumenti.

Il documento si fonda sulla normativa vigente e sulle buone pratiche amministrative adottate dalla Pubblica Amministrazione ed è integrato da tutte le procedure interne e *policy* definite dal CREA, fra le quali la *Politica per la Sicurezza delle Informazioni* predisposta ai sensi della Direttiva (UE) 2022/2555 (NIS2) e del relativo recepimento nazionale.

## Finalità del documento

Il presente documento definisce e detta agli utenti specifiche regole e condizioni di utilizzo degli strumenti informatici attraverso:

- la definizione di regole e procedure uniformi da applicarsi in tutte le aree operative;

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

- l'indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- la definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dal CREA nel rispetto della normativa vigente;
- l'individuazione delle responsabilità degli utenti in caso di inosservanza di regole e prescrizioni.

## Contesto normativo

Il presente disciplinare è redatto in linea con la seguente normativa:

- Codice penale, reati informatici: accesso abusivo (art. 615-ter), frode informatica (art. 640-ter), danneggiamento di dati (art. 635-bis) e intercettazione illecita (art. 617-quater);
- L.300/1970 (Statuto dei lavoratori) - artt.4,7 e 8;
- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali, fra cui le "Linee guida per posta elettronica e internet" di cui alla deliberazione 13/2007;
- Provvedimento del Garante del 27 novembre 2008, integrato nel 2009, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- D.P.R. 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione);
- Regolamento (UE) 2016/679 (*General Data Protection Regulation*, di seguito GDPR);
- Parere 8 giugno 2017 dell'EDPB (acronimo inglese per Comitato Europeo per la protezione dati personali), in merito al trattamento dei dati personali dei lavoratori;
- DPR n. 81 del 2023 - codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D.lgs. n. 165/2001;
- Provvedimento del Garante n.364/2024 - Metadati e posta elettronica;

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

- “Buone pratiche di cybersecurity di base per i dipendenti delle PP.AA.” approvato dal Consiglio dei ministri il 23 luglio 2025.<sup>1</sup>

## Titolarità delle risorse informatiche

Il CREA è proprietario esclusivo degli strumenti informatici, dei dispositivi e delle risorse documentali messi a disposizione del personale per lo svolgimento delle attività istituzionali. Tutti i dati, le informazioni e i documenti pertinenti all'attività lavorativa trattati o conservati sui sistemi dell'Ente rientrano nella sfera organizzativa e gestionale del CREA.

È ammesso un uso personale occasionale e limitato degli strumenti e delle risorse del CREA.

Al termine del rapporto di lavoro o collaborazione, il personale è tenuto a riconsegnare i dispositivi e le risorse assegnate. Eventuali informazioni personali presenti sui dispositivi devono essere rimosse o separate secondo modalità concordate con l'Amministrazione, garantendo la conservazione dei dati e documenti di interesse lavorativo.

## Glossario e definizioni

**Amministratore di sistema (AdS):** figura professionale finalizzata alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figura equiparabile (amministratori di basi di dati, di reti, di apparati di sicurezza e di sistemi *software* complessi), individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;

**CREA:** Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria;

**File di log:** registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori;

**Help Desk:** supporto tecnico operativo e specifico organizzato per singolo servizio;

<sup>1</sup> consultabile al seguente link <https://www.acn.gov.it/portale/vademecum-dipendenti> trasmesso alla “Lista Crea” con mail dell'8 dicembre 2025.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

**NDA:** accordo di riservatezza con cui le parti si impegnano a mantenere confidenziali determinate informazioni;

**PEC:** un sistema di comunicazione con caratteristiche di sicurezza e certificazione della trasmissione, con valore legale equiparato alla raccomandata A/R, assicurato dai gestori del servizio per le comunicazioni tra caselle PEC;

**Pila software:** elenco di *software* installati o installabili sui dispositivi del CREA (*Office 365, Microsoft Defender, etc.*);

**Postazione di lavoro (PdL):** personal computer (desktop o portatile), monitor, tastiera, mouse e quanto altro messo a disposizione dal CREA a ciascun utente per l'espletamento dell'attività lavorativa;

**Rete:** l'infrastruttura fisica e logica che permette l'interconnessione degli apparati dell'Ente, per la trasmissione dati fra loro e con la rete internet;

**Service Desk:** centro di competenza per la gestione dei servizi IT orientati al CREA;

**Soggetto fiduciario:** (figura prevista dal Provvedimento del Garante per la protezione dei dati personali del 1° marzo 2007) dipendente dell'Ente, individuato tra il personale appartenente alla medesima struttura organizzativa o comunque funzionalmente collegato al titolare dell'*account*, previamente autorizzato al trattamento dei dati personali e vincolato da obbligo di riservatezza, incaricato esclusivamente di accedere alla casella di posta elettronica istituzionale del dipendente assente nei casi e con i limiti previsti dal presente Disciplinare;

**Strumenti informatici:** personal computer fissi o portatili, stampanti, programmi e prodotti *software*, apparecchiature per la comunicazione unificata (videoconferenza, telefonia, chat, messaggistica, social network, posta elettronica, condivisioni, accessi remoti, ecc.);

## Principi Generali

Gli strumenti informatici sono assegnati agli utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e comportamenti adeguati ai compiti assegnati e alle responsabilità connesse nel rispetto del Codice di comportamento dei dipendenti della

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

Pubblica Amministrazione, del Codice di comportamento del CREA e delle istruzioni condivise.

Nell'esecuzione della propria attività lavorativa, gli utenti sono tenuti a:

- effettuare la propria attività uniformandosi alle disposizioni del CREA e alle istruzioni condivise;
- mantenere un comportamento lecito e tale da non compromettere il buon nome del CREA;
- custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente al Service Desk, ogni danneggiamento, smarrimento o furto;
- mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
- astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività in caso di cessazione dal servizio;
- adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione anche accidentale, dei dati;
- garantire la corretta custodia di atti e documenti di lavoro. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito.

I trattamenti dei dati personali effettuati durante l'utilizzo del sistema informatico devono rispettare i principi di cui agli artt. 5 e 25, comma 2, del GDPR, in particolare:

- liceità, correttezza e trasparenza del trattamento nei confronti degli interessati;
- limitazione delle finalità con trattamento dei dati per scopi determinati, espliciti e legittimi;
- minimizzazione dei dati;
- esattezza e aggiornamento dei dati;
- limitazione della conservazione;
- integrità e riservatezza. I sistemi informativi e le procedure di trattamento devono essere progettati e gestiti nel rispetto dei principi (*privacy by design e privacy by default*)

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

## Regole per l'utilizzo dei sistemi informativi

All'inizio di qualsivoglia rapporto lavorativo, il CREA affida al personale i necessari strumenti informatici. Qualora il CREA valuti il venir meno dei presupposti alla base dell'autorizzazione all'uso degli strumenti informatici, tale autorizzazione sarà revocata.

La revoca può riguardare:

- utilizzo del computer o altri dispositivi;
- utilizzo dei servizi di *Office Automation*;
- accesso a internet;
- accesso ai servizi applicativi;
- accesso alle sale tecniche (*Data center*).

## Credenziali di accesso

L'accesso alle applicazioni del sistema informativo del CREA avviene attraverso autenticazione mediante:

- credenziali di dominio (es: Documentale, Demetra, Monitor, Juppiter, Missioni, etc.);
- credenziali personali specifiche per determinate applicazioni (Inaz, Acquisti in Rete, etc.);
- credenziali SPID, CIE ed eIDAS;

In molti casi è necessario effettuare più operazioni di accesso (c.d. *login*), tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali può richiedere un *account* specifico; in questi casi, il CREA assegna uno *username* univoco e *password* per l'accesso alla risorsa.

Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse;

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate ad altri soggetti.

In caso di diffusione accidentale anche solo presunta, le password devono essere immediatamente modificate e l'incidente va segnalato al Service Desk.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

Il sistema di controllo degli accessi prevede:

- composizione di password complesse, (lunghezza minima stabilita, caratteri speciali e/o numerici);
- modifica della password al primo utilizzo;
- validità minima e massima della password;
- impossibilità di riutilizzo delle ultime password utilizzate;
- blocco dell'utenza dopo un determinato numero di tentativi falliti;
- reset della password e riattivazione delle utenze disabilitate, secondo le procedure in vigore.

Al fine di aumentare il livello di sicurezza, il CREA ha scelto:

- di implementare un sistema di Autenticazione a Fattori Multipli (*Multi Factor Authentication - MFA*), richiedendo all'utente di dimostrare la propria identità oltre che con la *password* anche con una seconda forma di verifica.

I metodi disponibili sono:

- *APP Authenticator*;
- comunicazione mail ad un indirizzo secondario;
- SMS inviato a un telefono cellulare nella disponibilità dell'utente.

Le utenze ospiti (*guest*) che non accettano l'invito entro un (1) mese vengono automaticamente rimosse.

Le utenze ospiti (*guest*) che hanno accettato l'invito vengono automaticamente rimosse se sono inattive da almeno sei (6) mesi.

Le utenze non utilizzate per dodici (12) mesi vengono automaticamente disattivate.

## Utilizzo di applicazioni aziendali

L'accesso alle applicazioni del CREA e il loro utilizzo devono avvenire secondo le regole del presente Disciplinare, con riferimento ai diversi ruoli di responsabilità per le varie tipologie di utenza.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

All'atto della cessazione/interruzione del rapporto di lavoro, fermo restando la disabilitazione all'uso degli applicativi e delle funzionalità dei servizi CREA, vige l'obbligo di restituire le strumentazioni (pc portatili, tablet, cellulari, kit di firma elettronica, ecc.).

In caso di assegnazione temporanea del personale CREA presso altra Pubblica Amministrazione, la titolarità della casella di posta elettronica sul dominio del CREA potrà essere mantenuta nel rispetto delle disposizioni ai sensi del presente disciplinare.

### Accesso da paesi esteri

Il CREA limita l'accesso alle risorse dell'Ente qualora le richieste provengano da aree geografiche estere. L'utente che preveda di trovarsi in un paese estero può richiedere una deroga temporanea al Service Desk mediante l'apertura di un ticket da parte del responsabile del progetto o del Direttore/Dirigente.

### Postazione di lavoro

Le PdL sono gestite dai Sistemi Informativi e dagli uffici di competenza dei Centri di Ricerca.

A ogni utente è assegnata una sola PdL inserita nel sistema di MDM - Mobile Device Management (es.: Microsoft Intune). L'assegnatario della PdL è profilato senza diritti amministrativi; eventuali deroghe sono possibili solo previa richiesta motivata da Dirigenti/Direttori e autorizzazione dei Sistemi Informativi.

La PdL è provvista di software di sicurezza (*software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.*). L'utente deve:

- comunicare al CREA ogni anomalia o malfunzionamento del sistema antivirus;
- evitare di accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria PdL;
- non ostacolare l'azione *dell'antivirus* aziendale;
- non disattivare *l'antivirus* senza previa autorizzazione dei Sistemi Informativi.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

L'utente assegnatario della PdL è responsabile del suo corretto utilizzo. In particolare, è vietato:

- danneggiare la PdL e gli accessori/periferiche in assegnazione;
- consentire l'accesso a soggetti non autorizzati;
- apportare modifiche alle configurazioni della PdL che non siano state preventivamente richieste al *Service Desk* e autorizzate;
- effettuare in proprio attività manutentive o consentirle a soggetti non autorizzati;
- utilizzare strumenti volti a eludere i sistemi di protezione;
- creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informativo (*virus, trojan* etc.);
- utilizzare programmi e/o sistemi di criptazione/cifatura senza la preventiva autorizzazione dei Sistemi Informativi;
- installare software di cui il CREA non possieda la licenza, o versioni diverse rispetto a quelle autorizzate senza l'espressa autorizzazione dei Sistemi Informativi;
- copiare il *software* installato per uso personale;
- modificare (eliminare, o impostare una diversa durata) lo *screen saver* auto bloccante;
- modificare la configurazione della PdL per escluderla dal sistema di monitoraggio e applicazione delle *policy* di sicurezza MDM - Mobile Device management – Microsoft Intune;
- formattare, alterare o distruggere i *device* assegnati;

Per le PdL portatili, ove supportato dal dispositivo l'utente è tenuto ad attivare il servizio TPM per la cifratura del disco, a personalizzare il PIN di accesso di non meno di quattro (4) caratteri e a conservare il PIN. In caso di difficoltà gli utenti possono rivolgersi al *Service Desk* per il necessario supporto.

Le PdL portatili devono essere periodicamente verificate dal *Service Desk* per la corretta configurazione e l'aggiornamento delle patch di sicurezza.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

In caso di significativo rischio di compromissione o di sicurezza, i Sistemi Informativi possono richiedere all'utente lo spegnimento della PdL portatile ovvero bloccare il dispositivo da remoto fino al termine delle verifiche.

L'utente è tenuto ad informare immediatamente i dirigenti responsabili della struttura organizzativa di appartenenza, i Sistemi Informativi – *Service Desk* e il *Responsabile della Protezione dei Dati* anche ai sensi della procedura di gestione delle violazioni di dati personali (*Procedura Data Breach*), di qualsiasi danno, furto o perdita di apparati, *software* e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

Relativamente ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le PdL.

### Software a corredo

È definita la lista degli applicativi standard disponibili nel documento **allegato (1)** e riguarda tutti i dispositivi aziendali.

L'eventuale utilizzo di *software* di tipo portatile (che non richiedono installazione) o installabile con i soli permessi utente è nella completa responsabilità dell'utente, sia per gli aspetti di diritto di proprietà intellettuale, sia per quelli di sicurezza.

Non è permessa l'installazione di *software* aziendale CREA su dispositivi privati.

In caso di particolari necessità, l'installazione di ulteriori software può essere richiesta al Service Desk, che valuterà l'ammissibilità della richiesta.

### Navigazione internet

La navigazione internet è messa a disposizione come fonte di informazione per finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa.

Il DPR n. 81 del 2023 ha integrato le disposizioni del Codice di comportamento dei dipendenti pubblici anche con due nuovi articoli (11-bis e 11-ter) riguardanti l'utilizzo delle tecnologie informatiche e dei mezzi di informazione, qui sinteticamente menzionati (art. 11-bis). Pertanto, l'utente deve:

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

- garantire la sicurezza dei sistemi informatici, evitando comportamenti che possano compromettere dati o infrastrutture digitali;
- proteggere dati e informazioni dell'amministrazione, nel rispetto delle norme sulla riservatezza e sulla sicurezza informatica;
- assumere la responsabilità dell'uso corretto delle credenziali di accesso e delle risorse digitali.

Ogni utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare *internet* per fini leciti, astenendosi dai comportamenti oltraggiosi e/o discriminatori;
- trasferire sul proprio computer, mediante *download*, solo file che non incorrano in violazioni di diritti di proprietà intellettuale;
- non utilizzare *social network*, *forum*, *chat* e simili per scambiare informazioni riservate o lesive dell'immagine del CREA;
- navigare in modalità trasparente e non anonima;
- non accedere, a siti i cui contenuti non siano adeguati all'immagine del CREA.

Il CREA adotta soluzioni di sicurezza basate su filtri e decriptazione della navigazione (ad esclusione di determinate categorie ad esempio siti bancari, sanitari, ecc.).

I tentativi di accesso a tali siti (ad esempio siti malevoli, gioco d'azzardo, siti per adulti, etc.) vengono bloccati automaticamente.

Sono inoltre adottate tecnologie anti-malware per la scansione dei contenuti scaricati.

## Stampanti

Le stampanti multifunzionali CREA (stampe, fotocopie, scansioni) devono essere usate correttamente; in caso di malfunzionamento bisogna chiamare la manutenzione e astenersi da qualunque intervento sulle macchine.

Gli utenti devono porre particolare attenzione alla riservatezza delle informazioni trattate attraverso le diverse funzionalità consentite.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

Per soddisfare le esigenze di riservatezza il CREA può prevedere sistemi di stampa associati a utenze individuali (c.d. “stampa riservata”), con rilascio dei documenti subordinato all'autenticazione dell'utente presso il dispositivo; l'utilizzo di tali sistemi è obbligatorio per le stampe contenenti informazioni particolari o riservate.

Quando l'utente fotocopie un documento deve porre particolare attenzione nel ritirare anche l'originale e l'eventuale memoria esterna (es. chiavetta USB).

La scannerizzazione di documenti comporta l'invio del documento scannerizzato dalla casella di servizio della stampante alla casella dell'utente destinatario del relativo file. I file generati nella casella di servizio sono temporanei e vengono cancellati dal sistema entro ventiquattro (24) ore dal compimento delle operazioni.

L'uso improprio della casella di servizio, come l'accesso non autorizzato (es. *login* con credenziali altrui per scaricare documenti non propri), la manipolazione dei file generati, l'invio degli stessi a terzi non autorizzati, è vietato e, al pari di altre condotte, può comportare responsabilità disciplinari.

## Posta elettronica

Tutti gli utenti per i quali ne sia rilevata la necessità sono dotati di una casella di posta elettronica sul dominio @crea.gov.it;

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, come indicato in “Posta elettronica e UC Netiquette – AGID”, documento reperibile al seguente link <https://trasparenza.agid.gov.it/download/5535.html>.

Il sistema di posta elettronica prevede:

- la possibilità di imporre limiti all'utilizzo del servizio (numero dei destinatari, dimensione degli allegati, dimensione complessiva della casella di posta elettronica);
- la possibilità per l'amministrazione di richiedere l'apertura di liste di distribuzione con o senza moderatore;
- l'uso limitato della funzione *reply all*;
- la scansione automatica di sicurezza dei messaggi (anti – malware e anti- phishing);

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

- un sistema automatico di classificazione (spam o posta indesiderata);
- per i messaggi rivolti all'esterno dell'Ente, l'inserimento automatico di un *disclaimer privacy*. Non è consentito inserire *disclaimer* personalizzati;
- il testo del *disclaimer* dichiara la natura riservata del contenuto e invita chi ha ricevuto il messaggio per errore a cancellarlo e avvertire il mittente.

Nell'utilizzo del servizio l'utente ha l'obbligo di:

- apporre in calce ai messaggi di posta elettronica la firma con nome e cognome, la struttura di appartenenza con relativo indirizzo, e ove assegnato, il numero di cellulare aziendale;
- proteggere la *privacy* dell'interlocutore evitando di inoltrare messaggi altrui a terzi;
- inviare posta elettronica esclusivamente a proprio nome. Si ricorda che è considerato mittente il proprietario della casella da cui è inviata la e-mail anche in presenza di altri nominativi;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine del CREA o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare di rispondere a "catene di Sant'Antonio", appelli o richieste non pertinenti all'attività lavorativa in CREA;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi;
- non iscriversi, con l'indirizzo aziendale, a social network, mailing list o servizi di interesse personale;
- non diffondere, all'esterno del CREA, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa.

#### **Accesso alla casella di posta per assenza del titolare dell'account**

La casella di posta elettronica istituzionale è uno strumento di lavoro. L'accesso ai contenuti da parte di altri soggetti è di norma escluso ed è ammesso esclusivamente nei

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

casi e secondo le modalità previste nel presente Disciplinare (nomina di un fiduciario), al solo fine di garantire la continuità operativa in caso di assenza del titolare.

Il soggetto fiduciario è individuato tra il personale appartenente alla medesima struttura organizzativa, o comunque funzionalmente collegato al titolare, previamente autorizzato al trattamento dei dati personali e vincolato da obbligo di riservatezza.

Si prevedono due modalità:

- **nomina preventiva:** il titolare può designare preventivamente un soggetto fiduciario con atto scritto (**Allegato (2)**), reso conoscibile all'Ente ai fini dell'attivazione tecnica;
- **nomina straordinaria:** in assenza di nomina preventiva e in presenza di comprovate esigenze di servizio caratterizzate da necessità e urgenza, il soggetto fiduciario è individuato dall'Amministrazione su richiesta scritta e motivata del Dirigente dell'Ufficio o del Direttore di Centro al Service Desk;

L'accesso del soggetto fiduciario avviene esclusivamente in modalità di sola lettura, è limitato ai soli messaggi strettamente necessari alle attività istituzionali, è circoscritto al tempo indispensabile ed esclude qualsiasi consultazione sistematica o indiscriminata della corrispondenza non pertinente.

Le operazioni tecniche di abilitazione e accesso sono soggette a tracciabilità. Il sistema IT registra: data e ora di abilitazione e disabilitazione; identità del soggetto fiduciario; modalità di accesso; eventi di accesso; operazioni tecniche necessarie. Le registrazioni sono conservate per un periodo limitato e proporzionato alle finalità di sicurezza.

In caso di attivazione dell'accesso: se in base a nomina preventiva, l'interessato è informato al rientro in servizio; se in base a nomina straordinaria, l'Ente informa l'interessato senza ritardo, appena cessata l'assenza. Al rientro, il titolare richiede al *Service Desk* la disabilitazione di ogni abilitazione temporanea.

### Metadati nei sistemi di posta elettronica

I sistemi di posta elettronica e di collaborazione digitale adottati dall'Ente generano automaticamente metadati tecnici relativi alle comunicazioni, tra cui:

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

- indirizzi del mittente e dei destinatari;
- data e ora di invio;
- oggetto del messaggio;
- dimensione del messaggio.

Tali metadati sono trattati esclusivamente per finalità di sicurezza informatica, prevenzione di accessi abusivi e tutela dell'integrità dei sistemi, secondo le configurazioni tecniche previste da *Microsoft 365*, fornitore del servizio di posta elettronica, nominato responsabile del trattamento ai sensi dell'art. 28 GDPR.

È escluso ogni controllo sull'attività lavorativa del personale CREA.

In considerazione della configurazione di *Microsoft 365*, che prevede la conservazione dei metadati (dati personali quali: mittente, destinatario, *timestamp*, *IP*, oggetto, ecc.) per un tempo superiore rispetto a quello previsto dal Provvedimento del Garante n. 364 del 6 giugno 2024, di ventuno giorni (21), l'Ente ha avviato un percorso di adeguamento volto a verificare la conformità del trattamento ai principi di necessità, proporzionalità e minimizzazione. Prossimamente saranno attivate le procedure previste dall'art. 4 dello Statuto dei lavoratori, mediante accordo sindacale ovvero autorizzazione dell'Ispettorato Nazionale del Lavoro, e si provvederà ad effettuare una specifica valutazione dei rischi e, ove necessario, una valutazione d'impatto sulla protezione dei dati (DPIA), nonché a adottare le eventuali misure tecniche e organizzative conseguenti.

## PEC

L'utilizzo delle caselle PEC è coordinato dai Dirigenti o Direttori di Centro di riferimento. Le caselle PEC nominali devono essere utilizzate esclusivamente per motivi di ufficio in conformità alle regole del presente disciplinare e alle disposizioni impartite da Dirigenti o Direttori di Centro.

La PEC viene disattivata nel momento in cui l'utente termina la collaborazione con l'Ente.

## Disattivazione caselle di posta

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

La casella di posta individuale viene disattivata dal competente *Service Desk* al termine del rapporto in essere, previa immediata comunicazione all'Ufficio sistemi informativi. La proroga del mantenimento deve essere autorizzata dal Direttore generale.

### Servizi di comunicazione

I servizi di comunicazione comprendono *chat*, telefonia, videoconferenza e collaborazione sui documenti. L'utente che invita ospiti esterni si assume la responsabilità dell'invito ed è tenuto a comunicare in anticipo agli altri partecipanti la presenza di informazioni personali o sensibili.

La registrazione di riunioni e l'utilizzo di sistemi di intelligenza artificiale per la creazione di resoconti di riunione deve essere comunicata e accettata da tutti i partecipanti.

### Servizi cloud e spazi di condivisione

Gli spazi di condivisione (*file server on premise o in cloud*) devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo.

Le autorizzazioni di accesso e i documenti archiviati sono soggetti a verifiche periodiche. In caso di comprovato pericolo per la sicurezza, il CREA potrà procedere anche senza preavviso alla rimozione di file o applicazioni, dandone successiva comunicazione.

### Dispositivi di memorizzazione portatili

L'utilizzo di supporti di memorizzazione rimovibili deve avvenire con cautela ed esclusivamente per le attività lavorative. Al momento della connessione di un dispositivo esterno, l'utente deve assicurarsi che venga avviata la scansione automatica antivirus, senza interromperla e senza disconnettere il dispositivo durante la scansione. È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di dati, anche se cancellati, senza preventiva cancellazione sicura (Shredding).

I supporti rimovibili devono essere custoditi con diligenza e non lasciati incustoditi. Quando non più necessari, devono essere restituiti ai Sistemi Informativi o al referente informatico.

Entro il 2026 sarà obbligatoria la cifratura dei supporti esterni di memorizzazione rimovibili.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

### Strumenti di firma digitale

L'uso del kit di firma digitale autorizzato per figure dirigenziali, RUP e DEC, è strettamente personale e non cedibile a terzi.

## Gestione degli incidenti di sicurezza informatica

### Definizione e ambito di applicazione

Per "incidente di sicurezza informatica" si intende qualsiasi evento, verificato o sospettato, che comprometta o possa compromettere la riservatezza, l'integrità o la disponibilità dei sistemi informativi, dei dati o dei servizi del CREA.

Sono considerati incidenti di sicurezza informatica, a titolo esemplificativo e non esaustivo:

- accessi non autorizzati a sistemi, applicazioni o dati;
- infezioni da malware (virus, ransomware, trojan, ecc.);
- perdita, furto o smarrimento di dispositivi contenenti dati aziendali o personali;
- trasmissione accidentale di dati riservati a destinatari non autorizzati (c.d. *data breach*);
- attacchi di phishing o social engineering andati a buon fine;
- compromissione delle credenziali di accesso.

### Obblighi di segnalazione

Ogni utente che venga a conoscenza o abbia il sospetto di un incidente di sicurezza informatica è **obbligato a segnalarlo immediatamente** al Service Desk e al proprio Dirigente/Direttore di riferimento. Ove il fatto coinvolga dati personali, va informato senza ritardo anche il Responsabile della Protezione dei Dati (DPO).

La segnalazione deve contenere, per quanto possibile:

- descrizione sintetica dell'evento (cosa è successo, quando, dove);
- sistemi, dati o servizi coinvolti;
- eventuali azioni già intraprese.

### Gestione e risposta

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

La gestione degli incidenti di sicurezza informatica è coordinata dai competenti uffici dell'Amministrazione Centrale in base alle procedure definite che:

- effettuano una prima valutazione della gravità e dell'impatto;
- attivano le misure di contenimento (es.: isolamento di dispositivi, revoca di credenziali);
- coinvolgono il DPO in caso di possibili violazioni di dati personali, con valutazione della notifica al Garante ai sensi dell'art. 33 GDPR;
- documentano l'incidente di sicurezza informatica e le azioni intraprese per tracciabilità e analisi delle cause.

## Controlli e monitoraggi

I referenti informatici svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dal CREA e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali. Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del sistema informativo comportanti l'accesso a cartelle, file o archivi di altri utenti, gli amministratori sono tenuti a preavvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

A tal fine, il CREA utilizza sistemi automatizzati per la gestione dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici del CREA e delle informazioni ivi contenute.

I file di log relativi alla navigazione internet sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente e alle disposizioni adottate al riguardo dal CREA.

Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log relativi alla navigazione possono essere esaminati per finalità di sicurezza e manutenzione dei sistemi, ogni accesso è tracciato.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

Di seguito si illustrano i tempi di conservazione dei file di log ad oggi stabiliti.

<b>Tabella log e tempi di conservazione</b>			
<b>Sistema</b>	<b>Tipo log/metadati</b>	<b>Finalità</b>	<b>Tempo di conservazione</b>
Posta Elettronica	Metadati tecnici	Funzionamento e sicurezza	Secondo configurazione Microsoft 365
Firewall	Log traffico rete	Sicurezza della rete	3-6 mesi
Autenticazione	Log accesso utenti	Sicurezza e audit	Sei mesi
Amministratori	Log attività	Audit di sicurezza	Sei mesi

Tutti i controlli avvengono nel rispetto del CAD, della normativa in materia di tutela dei lavoratori e della protezione dei dati personali. L'amministratore di sistema può isolare immediatamente l'origine di anomalie anche senza preavviso, con successiva informativa all'utente. I referenti informatici sono autorizzati ad attivare sistemi di prevenzione di intrusioni e ricezione di elementi nocivi; il blocco automatico dei messaggi da parte dei sistemi di protezione non costituisce violazione della sfera privata.

### **Responsabilità e sanzioni**

La violazione del presente disciplinare e dei Codici di comportamento può comportare l'applicazione delle sanzioni disciplinari previste dal decreto legislativo 30 marzo 2001, n. 165 e s.m.i., dai contratti collettivi applicabili al personale in servizio e dal singolo contratto di lavoro.

Resta ferma la responsabilità civile, penale e contabile di ogni utente per fatti illeciti e/o danni derivanti da usi non consentiti degli strumenti informatici messi a disposizione dal CREA.

	<b>SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> DISCIPLINARE PER L'UTILIZZO DELLE RISORSE INFORMATICHE	<b>DISC</b>
	CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria	Rev. 1.1 del 02/07/2026

Il CREA ha il dovere di segnalare alle autorità competenti, per gli opportuni accertamenti e l'adozione dei relativi provvedimenti del caso, gli eventuali usi illeciti degli strumenti informatici, potenzialmente configurabili come reati informatici.

**Copia del documento, già trasmesso via posta elettronica agli utenti in data 02 luglio 2026, viene pubblicata sul sito istituzionale dell'Ente, nell'apposita sezione «Amministrazione trasparente - Disposizioni generali - Atti generali - Atti amministrativi generali».**