Politica per la qualità
e sicurezza delle informazioni
Fondazione ICSC

REV.	AGG.	DATA	DESCRIZIONE MODIFICA	REDATTA /MODIFICATA DA	VERIFICATA DA	APPROVATO DA
0	0	16/04/2025	Prima emissione	Giulia Manenti	Daniela Gabellini	CdA

Sommario

1. Premessa

Il Centro Nazionale si impegna a garantire la qualità e la sicurezza delle informazioni, dei dati e dei servizi offerti ai Soci, Partner e Stakeholder, in linea con la missione di promuovere innovazione responsabile, sostenibilità e collaborazione pubblico-privata nel settore HPC, Big Data, AI e Quantum Computing.

La politica “qualità e sicurezza delle informazioni” della Fondazione ICSC incarna il nostro impegno nel promuovere il successo attraverso la generazione di valore e il sostegno alla crescita economica, per soddisfare e superare le aspettative di tutti gli stakeholder.

In linea con le normative internazionali ISO 9001, ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, abbiamo implementato un sistema di gestione integrato che mira all'eccellenza nel miglioramento continuo e nella gestione della sicurezza dei dati e delle informazioni. Il sistema è progettato per proteggere il nostro patrimonio informativo, quello dei Soci e quello dei destinatari dei nostri servizi, garantendo l'accessibilità, l'integrità, e la riservatezza delle informazioni solo alle parti autorizzate, sia interne che esterne.

2. Principi fondanti

Qualità: Tutte le attività, i servizi e le infrastrutture sono progettati e gestiti secondo criteri di eccellenza, trasparenza e miglioramento continuo, con attenzione alle esigenze di Soci e Partner.

Sicurezza delle Informazioni: Il Centro adotta misure tecniche, organizzative e procedurali per garantire la riservatezza, l’integrità e la disponibilità delle informazioni, in conformità alle normative nazionali ed europee, quali ISO IEC 27001, ISO IEC 27017 e ISO IEC 27018, Regolamento Europeo per la protezione dei Dati, Direttiva Europea 2022/2555 (“NIS2”).

Responsabilità Etica e Sociale: L’innovazione tecnologica è guidata da principi etici, sociali e giuridici, con particolare attenzione alla proprietà intellettuale, all’impatto sociale e alla sostenibilità.

Protezione dei dati personali: Il Centro adotta misure tecniche, organizzative e procedurali per garantire il corretto adempimento del Regolamento Europeo per la protezione dei Dati sia in qualità di Titolare, sia di Responsabile che di Sub-Responsabile del trattamento; e il rispetto dei requisiti di:

- liceità, correttezza e trasparenza del trattamento nei confronti dell’interessato;
- limitazione della finalità del trattamento;
- minimizzazione dei dati;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione.

Rispetto delle normative: Il Centro garantisce la piena conformità alle normative vigenti nazionali ed europee applicabili. Particolare attenzione è rivolta al rispetto delle linee guida ufficiali, dei regolamenti attuativi e dei requisiti previsti dai Bandi di finanziamento pubblici e privati, assicurando così trasparenza, correttezza e legittimità nell’accesso ai fondi e nella realizzazione delle attività progettuali.

3. Governance e organizzazione

Hub Nazionale di Dati: Il Centro opera come banca dati nazionale, promuovendo la collaborazione tra istituzioni e attori della ricerca e innovazione, e garantendo la sicurezza e la tracciabilità delle informazioni.

Modello Collaborativo: La governance integrata pubblico-privata favorisce la corresponsabilità e la partecipazione attiva di tutti gli attori, con processi decisionali trasparenti e inclusivi.

Gestione della Proprietà Intellettuale: Procedure strutturate per la tutela, la valorizzazione e il trasferimento dei risultati scientifici e tecnologici, con accordi di riservatezza e strumenti operativi dedicati. Inoltre, si adottano misure preventive per evitare la perdita del diritto d'autore attraverso il monitoraggio costante dei software utilizzati, siano essi usufruibili online o su licenza, prestando particolare attenzione alle implicazioni derivanti dall'introduzione dell'intelligenza artificiale.

Rafforzamento del ruolo internazionale: Il Centro agisce come leva strategica per consolidare la posizione dell'Italia nel contesto scientifico e tecnologico europeo, partecipando attivamente all'individuazione delle priorità nazionali e contribuendo al posizionamento competitivo del Paese su scala internazionale, in linea con la visione integrata e collaborativa delineata dalla governance e dalle attività operative del Centro.

Dialogo istituzionale e policy making: Il Centro assume un ruolo di interlocutore privilegiato nei confronti delle istituzioni, partecipando attivamente alla redazione di policy, raccomandazioni operative e white paper nell'ambito delle attività dell'Osservatorio, con il coinvolgimento diretto di soci pubblici, privati e opinion leader di settore.

Accesso ai finanziamenti e semplificazione amministrativa: Si promuove la creazione di condizioni favorevoli per l'accesso a fondi e risorse, implementando processi amministrativi semplificati a supporto dello sviluppo di progettualità innovative.

Valorizzazione economica e sostenibilità: Il Centro persegue la generazione di valore economico attraverso un surplus finanziario proveniente da contributi ordinari, investimenti in titoli di Stato e fondi dedicati, adottando strategie di impiego finalizzate a garantire la sostenibilità economica nel lungo periodo.

Monitoraggio del ritorno dell'investimento (ROI): Viene realizzata una valutazione periodica del ROI delle attività, distinguendo tra investimenti infrastrutturali e progettuali, al fine di assicurare un impatto concreto e misurabile nel triennio di riferimento.

4. Formazione e sensibilizzazione

Ruoli, responsabilità e competenze: La sicurezza delle informazioni e dei dati personali è affidata esclusivamente a personale dotato delle necessarie competenze e qualifiche, libero da conflitti di interesse e condizionamenti, al fine di garantire una governance efficace, una gestione adeguata degli incidenti – inclusi i Data Breach –, il presidio delle situazioni di crisi e la continuità operativa della Fondazione.

Formazioni e sensibilizzazione interna: al fine di rafforzare la cultura della qualità, sicurezza delle informazioni e sulla protezione dei dati personali, con sessioni dedicate al sistema di gestione implementato e relative policy, procedure e regolamenti, sui rischi potenziali – sempre più frequenti e complessi – e le modalità per prevenirli.

Valorizzazione delle competenze: Percorsi strutturati che includono la mappatura e la valorizzazione delle competenze interne, la formazione continua e la promozione di programmi di upskilling e reskilling nei settori chiave quali HPC, AI, Big Data e Quantum, affiancati da tirocini e iniziative di qualificazione professionale.

Comunicazione e Trasparenza: Progetti di comunicazione integrata per promuovere la consapevolezza e la diffusione delle buone pratiche tra tutti gli stakeholder.

5. Sistema di gestione per la qualità e sicurezza delle informazioni

Accesso e Protezione dei Dati: Accesso regolamentato alle infrastrutture e ai dati, con policy trasparenti e secondo i principi del need to know e del least priviledge.

Valorizzazione e Trasferibilità: Procedure per la consultabilità e la riproducibilità dei risultati, favorendo il trasferimento tecnologico e la creazione di spin-off e start-up.

Filiera e responsabilità condivise: Il Centro assicura che anche la propria catena di fornitura e le tecnologie adottate rispettino i requisiti di qualità e sicurezza delle informazioni e dei dati personali. Gli standard attesi vengono comunicati e condivisi con tutti i collaboratori e partner, prevedendo una chiara e trasparente ripartizione delle responsabilità in materia di sicurezza delle informazioni trattate nell'ambito dei rapporti contrattuali, sempre in aderenza alla normativa vigente.

Procedure di Sviluppo Sicuro: Nell'ambito delle attività di progettazione e realizzazione di soluzioni tecnologiche, on premisis e in cloud, vengono adottate procedure di sviluppo sicuro che integrano controlli e verifiche secondo i principi della security by design e by default. Queste procedure prevedono la valutazione preventiva dei rischi, l'implementazione di best practice riconosciute a livello internazionale e il ricorso a strumenti di analisi del codice e test di sicurezza, al fine di prevenire vulnerabilità e garantire la protezione delle informazioni trattate. L'adozione di tali misure si inserisce in un quadro di gestione integrata della qualità e della sicurezza, assicurando che ogni nuovo sviluppo sia allineato agli standard della Fondazione e contribuisca alla tutela dei dati e alla resilienza operativa.

Gestione del Rischio: Valutazione e gestione proattiva dei rischi legati alla sicurezza delle informazioni e alla qualità dei servizi, mantenendo un atteggiamento recettivo nei confronti dei rischi e delle opportunità derivanti sia dal contesto esterno sia da quello interno. Questo approccio consente di aggiornare costantemente la comprensione dei possibili impatti sulle informazioni gestite dal Centro e di favorire una risposta tempestiva ed efficace.

Gestione degli incidenti: Prevenzione e valutazione e gestione proattiva dei rischi legati alla sicurezza delle informazioni e alla qualità dei servizi.
Il Centro reputa fondamentale comunicare tempestivamente agli enti competenti e alle parti interessate tutti gli eventi che possono avere un impatto significativo sulla sicurezza delle informazioni e dei dati personali, in conformità agli accordi contrattuali e alle normative nazionali e internazionali vigenti. Si adottano misure fisiche e tecnologiche adeguate per la prevenzione degli incidenti, unitamente alla predisposizione di piani di risposta specifici per la gestione di crisi, incidenti e data Breach – o potenziali tali – al fine di assicurare la continuità e la protezione delle informazioni e dei dati personali e si garantisce la conservazione delle registrazioni necessarie per la ricostruzione degli eventi e delle relative cause.

Cloud: Controlli di Sicurezza aggiuntivi, in riferimento alla protezione dei personali e proprietari, in linea con gli standard adottati, tra cui:

- Chiara definizione delle responsabilità tra il fornitore di servizi cloud e la Fondazione, assicurando che entrambe le parti comprendano e rispettino i loro obblighi per mantenere la sicurezza dei dati;
- Gestione delle Operazioni in Cloud, stabilendo procedure dettagliate per la gestione sicura delle operazioni in ambienti cloud, inclusa la configurazione e il mantenimento dei servizi cloud.
- Gestione dell'interfaccia di rete, la segregazione in cloud, e la virtualizzazione sicura.

KPI e Audit: Introduzione di indicatori chiave di prestazione (KPI) e audit periodici, anche attraverso enti di certificazione qualificati, per monitorare l'efficacia delle misure adottate e garantire il miglioramento continuo.

Revisione per il miglioramento continuo: integrare i requisiti del sistema di gestione per la qualità, sicurezza delle informazioni e dei dati personali all'interno dei processi della Fondazione, mantenendo il sistema di gestione sempre aggiornato, monitorato e teso al miglioramento continuo, rappresenta un elemento cardine per garantire la protezione gli obiettivi del Centro. Questo approccio assicura che le procedure operative siano allineate alle migliori pratiche e alle normative vigenti, favorendo una cultura organizzativa orientata alla responsabilità e al miglioramento costante.

6. Impegno e responsabilità

L'impegno aziendale si traduce in particolare nel:

- Monitorare e rivedere regolarmente il nostro sistema di gestione per affrontare nuove minacce, soddisfare requisiti legali e normativi, e gestire efficacemente i rischi.
- Diffondere i nostri obiettivi di qualità e sicurezza per promuovere la condivisione di informazioni e il miglioramento continuo.
- Proteggere le informazioni da minacce significative, garantendo che i servizi forniti riducano i rischi per la sicurezza delle informazioni.
- Assicurare che i requisiti di riservatezza dei contratti siano adeguatamente analizzati e che le attività siano organizzate per rispettare le richieste di chi usufruisce del nostro servizio.
- Valutazioni e Audit Regolari tramite con audit specifici per i servizi cloud per identificare e mitigare i rischi emergenti.
- Mantenendo la politica delle qualità e sicurezza informazioni aggiornata in riferimento agli obiettivi annuali che l'azienda si pone, e che direzione in relazione anche agli ultimi sviluppi e le migliori pratiche nel settore dei servizi cloud, garantendo che le strategie di sicurezza siano all'avanguardia.
- Formazione continua, assicurando che tutto il personale sia consapevole e competente su come mantenere la qualità, garantire la compliance normativa e proteggere efficacemente i dati, in particolare per gli ambienti Cloud.

Tutti i Soci, Partner e Collaboratori del Centro Nazionale sono chiamati a rispettare e promuovere la presente Politica, contribuendo attivamente al raggiungimento degli obiettivi di qualità e sicurezza delle informazioni.

7. Validità

Il presente documento è valido immediatamente dopo la pubblicazione.

La Politica per la Qualità e Sicurezza delle Informazioni è verificata annualmente in sede di Riesame di Direzione.

Il Direttore Generale

Daniela Gabellini