UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA

AREA FORMAZIONE, RICERCA,
PIANIFICAZIONE E VALORIZZAZIONE
DELLE CONOSCENZE

LINEE GUIDA IN MATERIA DI SICUREZZA PER LA RICERCA

Approvato dal Senato Accademico in data 22 settembre 2025
Approvato dal Consiglio di Amministrazione in data 29 settembre 2025

Sommario

1. Definizioni 1
2. Principi 1
3. Compiti dei responsabili di attività 2
4. Protezione dei dati e cybersecurity 2
5. Beni e tecnologie a rischio dual use 3
6. Collaborazioni, sovvenzioni, contratti e donazioni 3
7. Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi . 3
8. Misure di sicurezza per i viaggi all'estero 4
9. Visite di personale esterno alle istituzioni di ricerca 4

1. Definizioni

Per Collaborazioni esterne e fonti di finanziamento esterne si intendono:

- collaborazioni con soggetti/istituzioni esterni all'Unione Europea o non appartenenti a istituzioni internazionali riconosciute tramite trattati;
- collaborazioni con soggetti non appartenenti a istituzioni pubbliche;
- finanziamenti provenienti da istituzioni esterne all'Unione Europea o non appartenenti a istituzioni internazionali riconosciute tramite trattati;
- Finanziamenti provenienti da soggetti privati.

Per Sicurezza e integrità della ricerca, così come definito in ambito G7 Sigre, si intende:

- Security of research means protecting research methods, data, and results from theft, misuse, inappropriate exploitation, and other forms of misconduct.
- Integrity of research, which is the direct product of integrity of researchers, is about sticking to professional values, principles, and practices that keep research honest, responsible, and societally impactful.

La definizione è in linea con quanto definito nella Raccomandazione del Consiglio dell'Unione Europea del 23 maggio 2024 in cui la "sicurezza della ricerca" è definita come "l'anticipazione e la gestione dei rischi relativi:
a) al trasferimento indesiderato di conoscenze e tecnologie critiche che possono compromettere la sicurezza dell'Unione e dei suoi Stati membri, ad esempio se deviate verso usi militari o di intelligence in paesi terzi;
b) a ingerenze malevole nella ricerca, che possono sfociare in una sua strumentalizzazione da parte di paesi terzi con lo scopo, tra l'altro, di creare disinformazione o incoraggiare l'autocensura tra studenti e ricercatori, violando la libertà accademica e l'integrità della ricerca nell'Unione;
c) a violazioni dell'etica o dell'integrità, in cui le conoscenze e le tecnologie sono utilizzate per reprimere, violare o minare i valori e i diritti fondamentali dell'Unione, quali definiti nei trattati."

2. Principi

Le linee guida si basano sui seguenti principi:

<u>Consapevolezza e comunicazione</u>
L'Ateneo dovrà fornire comunicazioni tempestive ed efficaci al personale ricercatore, al personale tecnico e amministrativo, nonché ai collaboratori e agli studenti, per aumentare la consapevolezza e fornire informazioni sull'influenza indebita da parte di eventuali attori potenzialmente malevoli (governi ed entità straniere e/o estranee al sistema nazionale della ricerca). Queste comunicazioni includono (ad esempio) informazioni su: azioni che i ricercatori possono intraprendere per mitigare possibili criticità; sui referenti a cui rivolgersi per assistenza; requisiti e responsabilità per la segnalazione, la divulgazione, il

controllo del trasferimento di conoscenze e tecnologie e altri controlli di sicurezza previsti dalle norme nazionali o europee.
L'Ateneo dovrà pubblicare e distribuire periodicamente newsletter sulla sicurezza riguardanti temi quali, a titolo di esempio, i rischi provenienti dall'estero e la preparazione per viaggi internazionali; organizzare seminari e presentazioni su integrità e sicurezza della ricerca rivolti ad audience specifiche (tesisti, dottorandi, ricercatori senior, project leaders, leadership accademiche ecc.).
L'Ateneo dovrà creare e mettere in evidenza nei siti web istituzionali pagine con link e informazioni su una vasta gamma di argomenti, quali: impegni di ricerca internazionali e collaborazione globale, influenze e interferenze indebite (per esempio, ma non solo, di governi stranieri) e mitigazione dei relativi rischi. Il sito web deve servire anche come 'sportello unico' per accedere alle politiche e pratiche dell'istituzione in tema di integrità e sicurezza della ricerca, alle relative comunicazioni e informazioni, alle linee guida, nonché ai requisiti definiti dalle istanze nazionali (Governo, Ministeri, ecc.).

Promozione del confronto nella comunità
L'Ateneo dovrà promuovere discussioni durante le riunioni degli organi di governo dell'istituzione e della comunità di ricerca (ricercatori e personale tecnico e amministrativo coinvolto), favorire incontri regolari a livello delle strutture interne (dipartimenti, istituti, divisioni ecc.) sui vari aspetti della integrità e sicurezza della ricerca.

Formazione
L'Ateneo dovrà organizzare moduli formativi su tematiche quali: integrità e sicurezza della ricerca, linee di condotta per viaggi e soggiorni all'estero, linee di condotta in presenza di visitatori nelle strutture, protezione dei dati e cyber-security, attività soggette a controllo delle esportazioni, protezione della proprietà intellettuale.

3. Compiti dei responsabili di attività

I responsabili di progetti di ricerca, programmi di collaborazione scientifica e didattica, attività di ricerca o innovazione commissionata, o conto terzi o spin off sono tenuti, prima dell'avvio della loro attività ad effettuare un'analisi del rischio in materia di sicurezza secondo tre possibili categorie di criticità, cioè quelle connesse:
a) all'ambito scientifico o tecnologico nel quale si colloca l'attività;
b) alle persone e alle istituzioni con cui si collabora;
c) alle entità che finanziano le attività;
d) alle persone che saranno ospitate durante lo svolgimento delle attività.

4. Protezione dei dati e cybersecurity

In materia di consapevolezza di rischi informatici nel contesto delle attività di ricerca scientifica occorre informare e formare ricercatori, studenti e personale amministrativo e tecnico sulla sicurezza informatica di base, sulle misure di protezione dei dati e sulle implicazioni della cybersecurity nella protezione delle attività di ricerca.

Si sottolinea l'importanza che tutte le attività di trattamento di dati personali connesse alle attività di ricerca scientifica vengano condotte nel pieno rispetto del Regolamento Generale per la Protezione dei Dati (GDPR, - Regolamento UE 2016/679).
Anche in questo ambito è opportuno condurre una analisi per la valutazione del rischio cyber associato alle attività di ricerca scientifica per adottare misure per la sicurezza informatica delle attività di ricerca e la prevenzione delle violazioni interne proporzionate al livello di rischio, alla criticità della specifica attività e alle altre informazioni di contesto.
È necessario monitorare i cambiamenti normativi e adottare pratiche di miglioramento continuo, con particolare riferimento alle norme comunitarie e nazionali, in collaborazione con le autorità competenti e il centro nazionale per la sicurezza e l'integrità della ricerca.

5. Beni e tecnologie a rischio dual use

I beni e le tecnologie che hanno la caratteristica di essere stati progettati per applicazioni civili ma che potrebbero eventualmente essere malversati in applicazioni belliche/nucleari in grado di sfuggire al monitoraggio dedicato a questo tipo di applicazioni sono regolamentati a livello comunitario e nazionale.
L'attività di ricerca, costantemente innovativa, è particolarmente esposta a processi di trafugamento e/o esportazione non autorizzata di beni e tecnologie. Inoltre, vi è anche la possibilità che entità ed organismi, estranee agli obiettivi pacifici della ricerca, siano interessate a raccogliere informazioni, conoscenze e materiale scientifico eventualmente utilizzabili in applicazioni non monitorate o vincolate da stati di embargo internazionale.

6. Collaborazioni, sovvenzioni, contratti e donazioni

È necessario avviare un'analisi del rischio anche per l'analisi di progetti, collaborazioni, contratti, accordi, sovvenzioni e donazioni, ogniqualvolta siano coinvolte entità esterne (si veda definizione iniziale). L'analisi dovrà includere il controllo delle eventuali esportazioni di tecnologie, la valutazione dei termini e condizioni delle sovvenzioni e la potenziale generazione e trasmissione all'esterno di dati o informazioni sensibili.

7. Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi

Un Conflitto di Interesse (COI) indica qualsiasi circostanza in cui gli interessi personali, professionali, finanziari o di altro tipo di un individuo (inclusi i membri immediati della sua famiglia) possono potenzialmente o effettivamente divergere, o possono essere ragionevolmente percepiti come potenzialmente o effettivamente divergenti, dai suoi obblighi professionali verso l'istituzione di appartenenza e dagli interessi dell'istituzione stessa. Un COI può esistere ogniqualvolta un osservatore indipendente possa ragionevolmente mettere in dubbio che le azioni o decisioni professionali dell'individuo, inclusa la condotta etica e obiettiva di studi, ricerche o attività cliniche, siano influenzate da considerazioni di guadagno personale, finanziario o di altro tipo. Le situazioni di COI si possono instaurare qualora il singolo ricercatore abbia interessi scientifici, finanziari o didattici con soggetti esterni all'istituzione di appartenenza. In questo ambito rientrano

affiliazioni, relazioni e interessi che possono entrare in conflitto con le responsabilità del ricercatore verso la propria istituzione. A titolo di esempio, si menziona la partecipazione a programmi di reclutamento, l'attribuzione di posizioni accademiche, le collaborazioni (anche a titolo non retribuito), il ruolo di "principal investigator" in progetti in cui non è coinvolta l'istituzione di appartenenza.

8. Misure di sicurezza per i viaggi all'estero

L'Ateneo dovrà sviluppare o aggiornare vademecum per viaggi internazionali e prevedere un registro per tenerne traccia e assicurarsi che i ricercatori ne abbiano preso visione prima di intraprendere un viaggio all'estero, fornire briefing sulla sicurezza personalizzati, se necessario, per destinazioni o scopi del viaggio con margini di criticità non trascurabili.

9. Visite di personale esterno alle istituzioni di ricerca

L'Ateneo dovrà sviluppare o aggiornare regolamenti per disciplinare visite di personale esterno nelle istituzioni di ricerca. Prevedere registri per l'accesso al fine di tenere traccia di elementi quali: visitatore/i, scopo della visita, personale interno incontrato, durata. prima della visita. Incentivare la formazione del personale esterno.