

## LINEE GUIDA PER LA GESTIONE DELLE INFORMAZIONI E DEI DATI CONFIDENZIALI

### Premessa

Le presenti linee guida hanno per oggetto le indicazioni operative per i ricercatori UniCT, relative al trattamento e la conservazione delle informazioni confidenziali, trasmesse da imprese o enti terzi ad UniCT nell'ambito di un accordo di riservatezza preliminare ad attività di ricerca o sperimentazione in comune o per conto terzi.

Non tutte le ricerche, né tutti gli scambi di informazioni richiedono la sottoscrizione preliminare di un accordo di riservatezza. Esso è necessario solamente per quelle informazioni, dati, ecc. che la parte concedente fornisce all'altra e che siano da questa ritenute confidenziali perché hanno un valore economico, per cui la loro rivelazione oltre lo stretto indispensabile rischia di provocare danni.

Pertanto, è indispensabile definire preliminarmente se le informazioni che vengono trasmesse ad UniCT siano effettivamente da considerare confidenziali e quali aspetti riguardino, al fine di evitare l'assunzione di obblighi non necessari e/o aventi contenuto impreciso, e in quanto tali suscettibili di successive controversie.

### Intestataro dell'accordo

Il ricercatore UniCT può sottoscrivere in prima persona accordi di riservatezza con enti esterni, ai vari fini di una conduzione di uno scambio informativo o collaborazione informale. Qualora operi in tal modo, il ricercatore non potrà spendere il nome di UniCT, né UniCT assumerà alcuna responsabilità, essendo gli obblighi assunti a titolo esclusivamente personale.

Qualora invece l'accordo coinvolga UniCT, esso sarà sottoscritto dal Rettore o dal Direttore di Dipartimento, a seconda dell'ambito di interesse, ed UniCT sarà a tutti gli effetti parte contrattuale.

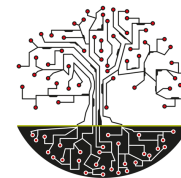
### Obbligazioni derivanti dall'accordo

La sottoscrizione dell'accordo da parte di UniCT non esonera i ricercatori interessati dalle proprie responsabilità. I ricercatori coinvolti in attività relative allo scambio informativo o alla ricerca che impiega le informazioni confidenziali ricevute dalle aziende si attengono alle presenti Linee guida.

### Il Gestore UniCT delle informazioni confidenziali

Il ricercatore interessato allo scambio di informazioni confidenziali ricoprirà il ruolo di *Gestore UniCT delle informazioni confidenziali*. Egli sarà responsabile delle informazioni riservate trasmesse dall'impresa o dall'ente terzo, avendo cura di definire come le stesse dovranno essere trasmesse, utilizzate e conservate all'interno di UniCT, quali persone potranno avere accesso alle stesse (tra dipendenti e non) e con quali modalità.

Il Gestore delle informazioni confidenziali:



sottoscriverà anche in proprio gli accordi di riservatezza o i contratti di ricerca che intende sottoporre alla firma dei Direttori di Dipartimento o del Rettore per adesione all'accordo e assunzione delle obbligazioni scaturenti da tale accordo;

potrà delegare le attività in questione a persona di sua fiducia, ma rimarrà comunque responsabile dell'operato di quest'ultimo per omessa vigilanza;

dovrà aver cura di far sì che ogni persona a cui vengano trasmesse informazioni confidenziali abbia sottoscritto un apposito impegno alla riservatezza, secondo il modello che sarà fornito dall'Ufficio brevetti, ovvero abbia controfirmato direttamente l'accordo di confidenzialità.

### **Trasmissione delle informazioni**

Le informazioni devono essere trasferite da parte di personale autorizzato dall'impresa o dall'ente terzo esclusivamente al Gestore delle informazioni confidenziali di UniCT, o a personale delegato.

Il trasferimento può avvenire tramite supporto fisico (hard disk, chiavetta USB, ecc.). In tal caso, il Gestore è responsabile della custodia di tale supporto fino al completamento dell'attività (v. "Conservazione").

È altresì possibile utilizzare il trasferimento via email, purché tramite un indirizzo di posta elettronica ufficiale dell'Università degli Studi di Catania. I destinatari della mail saranno esclusivamente persone già autorizzate alla ricezione delle informazioni confidenziali; i dati dovranno essere trasmessi preferibilmente attraverso file accessibili mediante codice/password (questi ultimi da non comunicare nel testo di mail).

Le stesse modalità utilizzate dall'impresa o ente terzo per trasmettere i dati ad UniCT potranno essere adottate dai ricercatori per comunicare tra di loro e con il personale autorizzato dell'impresa o ente terzo.

In caso contrario, altre modalità di trasmissione saranno opportunamente concordate con l'impresa o ente terzo.

### **Registrazione**

E' opportuno che l'ingresso dell'informazione venga annotato sinteticamente in una mail (da inviare alla controparte) che servirà da documentazione dell'avvenuta ricezione delle informazioni e dei dati, con indicazione specifica di ciò che deve essere considerato tra il materiale inviato come confidenziale e del personale autorizzato al trattamento dei dati e relativi recapiti.

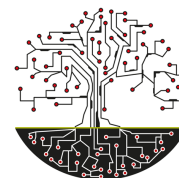
### **Conservazione**

I dati possono essere conservati:

- in formato cifrato, con almeno una chiave/codice/password;
- in chiaro, soltanto su supporti non connessi stabilmente alla rete (ad es. su hard disk esterni o sistemi di storage dipartimentali e/o d'Ateneo), tenuti in luoghi che ne garantiscano la riservatezza, con restrizioni adeguate e chiavi di accesso del solo personale autorizzato;
- in chiaro sui servizi cloud d'Ateneo, limitando l'accesso agli utenti associati allo specifico progetto.

### **Trattamento**

E' sconsigliato l'utilizzo di software che comporti la trasmissione online di dati confidenziali. Esempi non esaustivi sono tutti i software in modalità cloud ove non sia garantita la riservatezza dei dati.



I risultati dell'elaborazione devono essere conservati con gli stessi metodi sopra indicati, a meno che siano stati pensati ed eventualmente approvati per la pubblicazione, secondo quanto stabilito dalle stesse obbligazioni di riservatezza.

### **Doveri del personale autorizzato**

Il personale autorizzato (strutturato e non strutturato) all'accesso ai campioni e ai dati deve sottoscrivere per accettazione specifici impegni di riservatezza, secondo un modello fornito dall'Ufficio Brevetti.

Al termine dell'utilizzo delle informazioni riservate, il personale dovrà mantenere il rispetto dei doveri in materia di sicurezza degli accessi e mantenimento della riservatezza sulle informazioni.

Ogni caso di furto o altro evento in grado di violare la riservatezza delle informazioni di cui si venga a conoscenza, dovrà essere tempestivamente comunicato alla Direzione di Dipartimento per le opportune iniziative di salvaguardia o, se possibile, di contenimento del danno.