



UNIVERSITÀ  
DI SIENA  
1240

AREA ORGANIZZAZIONE  
E SISTEMI INFORMATIVI

Circolare

Classificazione: I/5

N. allegati: 1

Al personale docente  
Agli assegnisti di ricerca  
Agli studenti, ai dottorandi, agli specializzandi  
Al personale tecnico-amministrativo  
Ai collaboratori

**Oggetto: gestione delle credenziali di autenticazione per i servizi informatici dell'Ateneo**

Per ottemperare alle normative vigenti e migliorare il livello di sicurezza dei sistemi informativi dell'Università, si è reso necessario provvedere alla definizione delle procedure per la gestione delle credenziali di autenticazione per i servizi informatici dell'Ateneo.

Il Regolamento generale sulla protezione dei dati personali ("GDPR") impone la definizione di contromisure atte a minimizzare la possibilità del furto di dati ("data breach") e le eventuali conseguenze.

Risulta pertanto necessario adottare ogni strategia possibile per minimizzare ogni "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella comunità"<sup>1</sup> e per ottemperare alle tempistiche indicate agli articoli 33 e 34 del GDPR e garantire la libertà delle persone e la protezione dei loro dati personali.

È quindi necessario adottare una *password policy* di Ateneo che definisca le procedure e i processi per la gestione delle *credenziali di autenticazione*, come dal "considerando 83" del GDPR: "Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale."

Come riferimento tecnico per i "requisiti minimi delle credenziali di autenticazione" è stata considerata la direttiva del Presidente del Consiglio dei ministri 1 agosto 2015 "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"<sup>2</sup>.

<sup>1</sup> Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009

<sup>2</sup> [https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/misure\\_minime\\_di\\_sicurezza\\_v.1.0.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf)



UNIVERSITÀ  
DI SIENA  
1240

AREA ORGANIZZAZIONE  
E SISTEMI INFORMATIVI

La normativa europea (GDPR) obbliga gli enti e le aziende ad attuare il paradigma del *security by design* per lo sviluppo e la distribuzione delle piattaforme informatiche. Principio peraltro contemplato anche nelle precedenti normative italiane così come nel CAD – *Codice dell'amministrazione digitale* – e nelle relative misure minime di sicurezza.

Per poter quindi ottemperare ai requisiti indicati e migliorare la sicurezza nella gestione delle credenziali abbiamo implementato una serie di procedure all'interno del portale "[my.unisi.it](https://my.unisi.it)" per la gestione, manutenzione e verifica delle stesse.

Il documento allegato descrive le misure di sicurezza, le procedure e gli obblighi connessi all'uso e alla gestione delle credenziali di autenticazione per i servizi informatici dell'Ateneo.

Cordiali saluti.

Siena, data della firma digitale

Il responsabile dell'Area

Enrico Brighi

*(documento sottoscritto con firma digitale)*

ALLEGATI

1. Manuale gestione credenziali di autenticazione