



**UNIVERSITÀ  
DI SIENA**  
1240

# **PASSWORD POLICY DI ATENEO**

**COME FARE PER...**



UNIVERSITÀ  
DI SIENA  
1240

## INTRODUZIONE

---

Le credenziali di Ateneo permettono l'accesso ai servizi informatici offerti dall'Università, come la posta elettronica, la rete wireless, alla VPN, i servizi online per gli studenti, i servizi U-GOV, le postazioni di lavoro.

Risulta dunque evidente che la robustezza della password e le buone pratiche di conservazione della stessa siano fattori determinanti nella protezione dei propri dati personali e nella protezione dei dati della nostra organizzazione.

## COME FACCIAMO A SAPERE SE LA MIA PASSWORD È SICURA

---

Per garantire un'adeguata sicurezza della password, ci sono alcuni parametri da rispettare:

- la lunghezza deve essere di almeno 8 caratteri alfanumerici (con lettere sia maiuscole che minuscole);
- non può coincidere con il nome utente;
- non deve contenere né il nome né il cognome;
- non deve essere all'interno di un elenco di password comuni;
- non deve essere già stata utilizzata in passato.

È buona norma cambiare periodicamente la password e, per questo, sarai avvisato con un promemoria di cambio password, nel caso fosse trascorso il tempo massimo di validità previsto dalla normativa (6 mesi dall'ultimo aggiornamento).

Le password sono conservate in modo cifrato (*hash*) all'interno dei server dell'Ateneo.

## MANTENERE SICURO L'ACCOUNT

---

Una password robusta è il primo passo per mantenere al sicuro le nostre credenziali di autenticazione, di cui siamo formalmente responsabili.

Tuttavia questo non è sufficiente a garantirne la sua sicurezza. Per questo consigliamo agli utenti di:

- non utilizzare la stessa password per più account su siti web diversi (es. su Google, Facebook



## UNIVERSITÀ DI SIENA 1240

- e Unisi), soprattutto se si utilizza il medesimo indirizzo e-mail;
- abbonarsi (gratuitamente) ad un servizio di verifica di compromissione del proprio indirizzo e-mail, come Firefox Monitor (<https://monitor.firefox.com>): in caso di violazione dei dati, si viene avvisati automaticamente;
  - non scrivere mai la password su post-it o altri luoghi accessibili a terzi: conviene utilizzare un password manager, come KeePassX (gratuito – <https://keepass.info>), dove conservare le varie credenziali.

### **RECUPERO IN CASO DI SMARRIMENTO**

---

Se non ricordi più le tue credenziali di accesso, è possibile effettuare la reimpostazione delle stesse attraverso un canale alternativo di comunicazione (es. e-mail privata) precedentemente comunicato.

Queste operazioni si effettuano attraverso il portale "[my.unisi.it](https://my.unisi.it)".

Nel caso tu non abbia comunicato il canale alternativo, potrai effettuare la procedura di recupero mediante identificazione diretta con il personale autorizzato, che può essere contattato tramite l'indirizzo [helpdesk@unisi.it](mailto:helpdesk@unisi.it) oppure chiamando lo 0577235000.

### **REIMPOSTAZIONE IN CASO DI BLOCCO ACCOUNT**

---

Nel caso vengano rilevate attività in violazione della normativa vigente e del regolamento contenente il disciplinare informatico dell'Università degli Studi di Siena, il tuo account potrà essere bloccato in via precauzionale dagli operatori autorizzati, fermo restando altri obblighi di legge.

Il blocco comporta l'impossibilità di utilizzare le credenziali per l'accesso ai servizi telematici dell'Ateneo. Pertanto dovrai procedere con la reimpostazione della password, seguendo la procedura indicata nel portale "[my.unisi.it](https://my.unisi.it)".



UNIVERSITÀ  
DI SIENA  
1240

## OBBLIGHI DELL'UTENTE

---

Ai sensi della normativa vigente, hai l'obbligo di custodire le tue credenziali di accesso con la massima diligenza, avendo cura di non divulgarle né cederle a terzi, per alcun motivo.

In caso di furto, smarrimento o perdita di esclusività, l'utente ha l'obbligo di effettuare la segnalazione nel più breve tempo possibile all'indirizzo [abuse@unisi.it](mailto:abuse@unisi.it).