



UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

LINEE GUIDA UTILIZZO DEL CLOUD

Approvato dal Consiglio di Amministrazione in data

LINEE GUIDA UTILIZZO DEL CLOUD

SOMMARIO

1.	SCOPO E CAMPO DI APPLICAZIONE	3
2.	RESPONSABILITÀ.....	3
3.	NORMATIVA DI RIFERIMENTO	3
4.	MODALITÀ DI ACCESSO E AUTENTICAZIONE PER GLI UTENTI	4
5.	REGOLE PER L'USO CORRETTO DEI SISTEMI.....	4
6.	REGOLE PER SEGNALAZIONI DI Malfunzionamenti e anomalie	6

1. Scopo e campo di applicazione

Il presente documento ha lo scopo di fornire agli utenti una guida chiara per un utilizzo responsabile, efficace e sicuro dei servizi cloud. Esso si applica a tutto il personale docente, amministrativo e tecnico, ai collaboratori esterni a vario titolo identificati nel sistema Identity di Ateneo nonché agli studenti che utilizzano i servizi cloud nell'ambito delle attività istituzionali.

Per informazioni sulla gestione dei servizi cloud fare riferimento alla “Politica di Gestione del Cloud” approvata dal Consiglio di Amministrazione nella seduta del 24/01/2025
<https://www.sicurezzaict.unimore.it/2025/01/29/politica-di-gestione-del-cloud/>

2. Responsabilità

La responsabilità primaria dell'applicazione delle regole previste dal presente documento ricade su ciascun utente, che è tenuto a rispettare scrupolosamente le disposizioni in materia di sicurezza e utilizzo corretto dei servizi cloud.

Ogni utente deve agire con consapevolezza e diligenza, adottando comportamenti adeguati a prevenire rischi e garantire la protezione delle informazioni.

In seconda istanza, la Direzione Sistemi Informativi e Assicurazione Qualità (DIAQ) è incaricata di vigilare sull'applicazione complessiva della presente guida, fornire supporto, effettuare controlli periodici e promuovere iniziative di sensibilizzazione e formazione in materia di sicurezza informatica.

La condivisione non autorizzata di informazioni riservate, così come la perdita colposa di dati personali o particolari (ex sensibili), può comportare conseguenze giuridiche per l'utente responsabile, incluse sanzioni civili e, nei casi più gravi, penali, in conformità alla normativa vigente.

3. NORMATIVA DI RIFERIMENTO

L'utilizzo dei servizi cloud all'interno dell'Ateneo deve avvenire nel pieno rispetto del Regolamento Generale sulla Protezione dei Dati (GDPR), delle normative ISO/IEC 27001, 27017, 27018, oltre che dei regolamenti interni dell'Ateneo.

Il GDPR impone che i dati personali siano trattati in modo lecito, corretto e trasparente, assicurando adeguate misure di protezione contro accessi non autorizzati, perdite, distruzioni o alterazioni. È responsabilità sia degli utenti sia dell'Ateneo garantire la riservatezza, l'integrità e la disponibilità delle informazioni personali.

Le norme ISO/IEC forniscono un quadro di riferimento internazionale per la gestione della sicurezza delle informazioni:

- La ISO/IEC 27001 definisce i requisiti per l'adozione di un sistema strutturato di gestione della sicurezza.
- La ISO/IEC 27017 fornisce specifiche linee guida per la sicurezza dei servizi cloud, con particolare attenzione alla gestione degli accessi e alla protezione dei dati durante l'elaborazione.
- La ISO/IEC 27018 introduce principi per la tutela dei dati personali nei servizi cloud pubblici, garantendo la protezione dei diritti degli interessati.

A livello interno, la Politica di Gestione del Cloud recepisce le normative e le buone pratiche sopra citate, con particolare riferimento alla conformità alla ISO/IEC 27017, alla ISO/IEC 27018 e alla Direttiva (UE) 2022/2555 (NIS 2), definendo principi e linee guida per un uso sicuro, consapevole e conforme dei servizi cloud nell'ambito delle attività dell'Ateneo

Modalità di accesso e autenticazione per gli utenti

Le piattaforme cloud autorizzate in Ateneo a cui è consentito l'accesso e l'utilizzo con le credenziali Unimore e su cui è possibile caricare file e documenti sono:

- Piattaforma Google Workspace: fornisce il servizio di posta elettronica istituzionale Gmail e l'accesso alla memorizzazione di documenti su Drive
- Piattaforma Microsoft 365: fornisce l'accesso alle app online, tra cui Teams per la didattica e la collaborazione, OneDrive per la memorizzazione di documenti, SharePoint per siti intranet. Comprende l'accesso alla piattaforma cloud pubblica Microsoft Azure (risorse di elaborazione, archiviazione, memorizzazione, trasmissione dati e interconnessione di reti, analisi, intelligence, apprendimento automatico, sicurezza e gestione delle identità, monitoraggio e gestione, servizi per lo sviluppo di applicazioni ecc.)
- Applicativi gestionali su piattaforma CINECA
- Spazio disco per backup su sistemi Lepida Google Workspace e Microsoft 365.

Le piattaforme sono gestite a livello centralizzato dalla DIAQ e garantiscono strumenti valutati sicuri e conformi per la gestione di dati, comunicazioni e collaborazione aziendale.

L'accesso è riservato agli utenti autorizzati tramite il sistema **Identity di Ateneo**, ovvero:

- Docenti;
- Personale tecnico-amministrativo;
-  Studenti in corso;
- Studenti alum, entro 3 anni dal conseguimento del titolo;
- Studenti pre-immatricolati: solo accesso al portale CINECA per la gestione della carriera (Esse3) e alle app di Microsoft 365 entro i 2 anni seguenti alla pre-registrazione e ai fini della fruizione della fruizione della didattica prima dell'immatricolazione;
- Collaboratori a vario titolo identificati nel sistema Identity di Ateneo;
- Ospiti (**guest**) su invito specifico.

Per accedere ai servizi cloud supportati, gli utenti eccetto quelli qualificati come Ospiti (guest) devono:

1. Autenticarsi via SSO con le proprie credenziali istituzionali nel portale dedicato.
2. Selezionare la piattaforma cloud richiesta (es. Microsoft 365, Google Workspace).
3. Accettare i termini d'uso e configurare eventuali impostazioni di sicurezza aggiuntive.

3.1. UTENTI GUEST

Gli utenti guest possono accedere solo ai servizi cloud di Microsoft 365 e **solo previa esplicita autorizzazione e invito da parte di un utente istituzionale**. L'accesso è limitato in termini di funzionalità e tempo, ed è regolato da permessi specifici definiti dall'Ateneo.

Per i guest:

- L'accesso avviene tramite invito personalizzato ricevuto via e-mail.
- È richiesta l'autenticazione con un account personale o del proprio ente di appartenenza (generalmente Google o Microsoft) associato all'invito.
- I guest sono tenuti ad accettare i termini d'uso specifici e a rispettare le condizioni di accesso temporaneo e limitato.
- L'account guest può essere disabilitato o revocato in qualsiasi momento per motivi di sicurezza o cessazione della collaborazione.

E' consentito, previa richiesta e autorizzazione, l'ingresso nel tenant Microsoft di utenti di altre organizzazioni in modalità "cross-tenant" quindi come ExternalUser.

3.2. RICHIESTA DI AUTORIZZAZIONE PER L'USO DI CLOUD DIVERSI

Eventuali necessità di accesso a piattaforme cloud diverse da quelle gestite dalla DIAQ devono essere concordate preventivamente con la Direzione della DIAQ e con il Direttore/Dirigente della propria struttura.

In particolare, al ricorrere di tale ipotesi, gli utenti devono presentare richiesta scritta alla DIAQ, avendo cura di specificare:

- la piattaforma che si intende utilizzare;
- le finalità d'uso;
- la tipologia di dati coinvolti.

La DIAQ valuterà la richiesta in base alla sicurezza, alla conformità normativa e alle esigenze operative dell'Ateneo, fornendo un riscontro formale sull'autorizzazione o eventuali indicazioni integrative.

4. Regole per l'Uso Corretto dei Sistemi

Gli utenti sono responsabili della corretta gestione delle proprie credenziali, dei dati e delle risorse cloud messe a disposizione dall'Ateneo. In particolare, devono:

- **Proteggere le credenziali di accesso**, mantenendole riservate e senza condividerle con terzi.

Comportamento da evitare: Scrivere la password su post-it visibili o condividerla tramite e-mail o chat.

- **Adottare password robuste**, conformi ai criteri aziendali, e aggiornarle periodicamente, preferibilmente ogni 90 giorni (ad esempio: Gv7!rP9@xL).

Comportamento da evitare: Usare password deboli come "123456" o non cambiarle per lunghi periodi.

- **Archiviare i documenti in modo ordinato**, utilizzando cartelle strutturate e condivise solo con persone autorizzate.

Comportamento da evitare: Salvare file importanti in cartelle disorganizzate o accessibili a chiunque.

- **Mantenere l'archiviazione entro le quote assegnate** avendo cura di cancellare file obsoleti, di prova, non più in uso anche archiviandoli localmente

Comportamento da evitare: Caricare più copie dello stesso file, utilizzare il cloud per backup di dispositivi, caricare file personali, utilizzare la posta elettronica come repository

- **Condividere dati e documenti esclusivamente con utenti autorizzati**, utilizzando sistemi sicuri, come link protetti da password o con scadenze temporali.

Comportamento da evitare: Condividere link aperti senza protezione o inviare documenti riservati a destinatari non autorizzati.

- **Seguire le policy aziendali sulla classificazione dei dati**, distinguendo correttamente tra dati pubblici, riservati e critici. Salvare contenuti sensibili in storage locali cifrati evitando di caricarli in cloud. Non usare parole offensive nei nomi dei file e non inserirle nei contenuti dei file, i contenuti che violano queste regole saranno automaticamente cancellati

Comportamento da evitare: Trattare dati particolari (ex sensibili) come se fossero pubblici o inviarli su canali non sicuri.

- **Se non debitamente autorizzati, utilizzare esclusivamente le piattaforme cloud autorizzate**, quali Google Workspace (in particolare scambiare documenti con Gmail e archiviare documenti su Drive tramite Drive personali o Drive condivisi) e Microsoft 365 (in particolare archiviare documenti su OneDrive o Sharepoint o scambiarsi documenti nelle chat o nei team creati su Teams)

Comportamento da evitare: salvare file aziendali su piattaforme non autorizzate come account personali di Dropbox, ecc.

- **Affidarsi ai sistemi di backup automatici configurati dalla DIAQ**, senza utilizzare soluzioni esterne non autorizzate.

Comportamento da evitare: Eseguire salvataggi manuali su chiavette USB o dischi esterni personali non protetti.

- **Segnalare tempestivamente eventuali anomalie, violazioni di sicurezza o perdite di dati** agli amministratori competenti e al CSIRT Unimore (csirt@unimore.it)

Comportamento da evitare: Ignorare e-mail sospette, accessi anomali o incidenti di sicurezza senza segnalarli immediatamente.

Regole per SEGNALAZIONI DI MALFUNZIONAMENTI E ANOMALIE

In caso di malfunzionamenti, anomalie di sistema, accessi sospetti, violazioni di sicurezza o smarrimento di dati, è fondamentale effettuare una segnalazione tempestiva.

Fare riferimento alla politica di Gestione degli incidenti informatici

<https://www.sicurezzaict.unimore.it/2024/07/16/pol101-politica-di-gestione-degli-incidenti-di-sicurezza/> approvata dal CdA.

Gli utenti devono segnalare le anomalie riscontrate in primo luogo al Referente di sicurezza della propria struttura.

Presso la DIAQ è attivo il supporto IT di II livello raggiungibile dal portale

<https://support.unimore.it>

In particolare, ogni incidente informatico deve essere segnalato prontamente al CSIRT

Unimore csirt@unimore.it

Le segnalazioni devono contenere una descrizione chiara del problema, la data e l'ora dell'evento, eventuali messaggi di errore ricevuti e, se possibile, screenshot utili a identificare la criticità. Il supporto tecnico prenderà in carico la richiesta e fornirà assistenza nel più breve tempo possibile.