UNIVERSITÀ
DEGLI STUDI
DI MILANO

*Carta dei Servizi*

# Direzione Generale - Staff di I livello
# Cybersecurity, Protezione Dati e Conformità

UNIVERSITÀ DEGLI STUDI DI MILANO

**Direzione Generale - Staff di I livello**
**Cybersecurity, Protezione Dati e Conformità**

***Sportello di orientamento all'utenza***

| | |
|---|---|
| *Descrizione* | Orientamento generale sulle modalità di richiesta di consulenze in ambito di sicurezza informatica e/o di protezione dati (anche personali) |
| *Destinatari* | Personale docente e tecnico, amministrativo e bibliotecario, studenti, dottorandi, specializzandi, borsisti, assegnisti, esterni |
| *Modalità di erogazione* | e-mail a: sportello.sicurezzaeprotezionedati@unimi.it |
| *Contatti* | Responsabile di Struttura<br>sportello.sicurezzaeprotezionedati@unimi.it |
| *Indicatori* | **Accessibilità:**<br>36 ore settimanali (orario 9-13 e 14-17)<br>**Tempestività:**<br>risposta entro 3 giorni lavorativi |
| *Link utili* | work.unimi.it/aree_protette/121679.htm |

***Gestione campagne malevole via email***

| | |
|---|---|
| *Descrizione* | Gestione segnalazioni di email potenzialmente pericolose ricevute. Gestione e neutralizzazione della campagna, comunicazione con gli utenti potenzialmente coinvolti tramite e-mail informative e avvisi sul portale di Ateneo, indicazioni sulle misure specifiche di sicurezza per gli utenti colpiti, con supporto via e-mail o eventuale contatto telefonico |
| *Destinatari* | Possessori di casella di e-mail su dominio @unimi.it, @studenti.unimi.it, @guest.unimi.it |
| *Modalità di erogazione* | e-mail a: sicurezza@unimi.it |
| *Contatti* | Capo Ufficio CERT e Gestione Incidenti<br>sportello.sicurezzaeprotezionedati@unimi.it |
| *Indicatori* | **Accessibilità:**<br>36 ore settimanali (orario 9-13 e 14-17)<br>**Tempestività:**<br>tempo medio di gestione della campagna e prime contromisure entro 1 giorno lavorativo |
| *Link utili* | Informazioni: work.unimi.it/servizi/security_gdpr/118546.htm<br>Avvisi: work.unimi.it/servizi/security_gdpr/118606.htm |

***Accesso remoto sicuro alle risorse di Ateneo – Servizio VPN***

| | |
|---|---|
| *Descrizione* | Gestione delle richieste di abilitazione di account per l'accesso sicuro, tramite VPN, ai servizi e alle risorse protette dall'esterno della rete di Ateneo o a servizi riservati sulla intranet.<br>La richiesta per i dipendenti in telelavoro o smart working deve pervenire dalla Direzione Risorse umane.<br>La richiesta per l'abilitazione al servizio VPN del personale tecnico amministrativo, per altre esigenze, e di fornitori delle strutture tecniche deve avvenire su richiesta del responsabile della struttura richiedente. I fornitori vengono contattati telefonicamente per la trasmissione delle credenziali di primo utilizzo.<br>Risposta a eventuali criticità di accesso al servizio VPN vengono fornite via e-mail. Per alcuni utenti possono essere richieste regole di accesso idonee alle specifiche esigenze. |
| *Destinatari* | Personale tecnico, amministrativo e bibliotecario, fornitori delle strutture tecniche |
| *Modalità di erogazione* | Per il personale tecnico, amministrativo e bibliotecario (Lavoro Agile e Telelavoro) è necessaria una comunicazione dalla Direzione Risorse umane e-mail a: vpn@unimi.it<br>Per il personale tecnico amministrativo e per i fornitori esterni le richieste devono essere inoltrate dai responsabili delle strutture tecniche. Per i fornitori esterni si dovranno indicare nella motivazione gli estremi e la data di scadenza del contratto.<br>Richiesta tramite Modulo Elixform<br>Supporto e-mail vpn@unimi.it |
| *Contatti* | Capo Ufficio Tecnologie di Sicurezza<br>sportello.sicurezzaeprotezionedati@unimi.it |
| *Indicatori* | **Accessibilità**<br>modulo 24 ore<br>**Tempestività**<br>abilitazione dell'utente entro 3 gg lavorativi |
| *Link utili* | Informazioni: work.unimi.it/servizi/security_gdpr/122956.htm |

***Data breach***

| | |
|---|---|
| *Descrizione* | Gestione e istruttoria, su segnalazione, di violazione di dati personali quali quelle ad esempio dovute a smarrimento di una memoria removibile, come un hard disk esterno o una pen-drive USB contenente dati, violazione di un account di posta elettronica, compromissione di un PC o di un server, criptazione di dati a seguito di attacco ransomware, pubblicazione non autorizzata di dati salvati all'interno del database di un sito web su internet |
| *Destinatari* | Personale docente e tecnico, amministrativo e bibliotecario, dottorandi, specializzandi, borsisti, assegnisti |
| *Modalità di erogazione* | e-mail a: violazione.dati@unimi.it<br>Segnalazione via email a violazione.dati@unimi.it di un evento di data breach; compilazione e invio del modulo disponibile online work.unimi.it/filepub/sicurezza_ict/Segnalazione_data_breach.pdf e gestione istruttoria in base alla tipologia di incidente |
| *Contatti* | Capo Ufficio Protezione dati, AUDIT e conformità normativa<br>sportello.sicurezzaeprotezionedati@unimi.it |
| *Indicatori* | **Accessibilità:**<br>36 ore settimanali (orario 9-13 e 14-17)<br>**Tempestività:**<br>Avvio verifiche e istruttoria entro 1giorno lavorativo, predisposizione per notifica al Garante della Privacy entro 72 ore ai sensi del Regolamento Ue 2016/679 (GDPR) |
| *Link utili* | Informazioni: work.unimi.it/servizi/security_gdpr/118592.htm |