Misure di protezione cybersecurity e protezione dati da osservare durante il lavoro agile

Sommario

Lavorare da Remoto in modo sicuro in 15 punti

1. **Utilizza le risorse messe a disposizione dall'Ateneo solo ed esclusivamente per lo svolgimento delle mansioni lavorative**

2. **Accertati di usare sempre la VPN fornita dall'Università**

3. **Configura una buona password sul router Wi-Fi di casa per garantire che il tuo traffico non possa essere intercettato facilmente**

4. **Utilizza sempre l'Antivirus fornito dall'Ateneo e verifica il suo costante funzionamento**

5. **Utilizza un profilo di accesso al pc dedicato al lavoro protetto da una credenziale robusta e imposta il blocco del computer quando ti allontani dalla postazione**

6. **Non collegare dispositivi esterni (penna USB, Hard Disk esterni) di cui non conosci la provenienza**

7. **Per salvare e o condividere dati utilizza sempre gli strumenti di Ateneo (es. Unimibox, Dataserver, ecc.) che garantiscono maggior affidabilità oltre che il backup dei dati. Non salvare documenti in archivi personali o su risorse cloud non autorizzate espressamente dall'Ateneo**

8. **Presta attenzione quando leggi le mail, evita di scaricare allegati o cliccare su link ricevuti in e-mail da mittenti sconosciuti. Evita di usare la casella di posta come archivio di dati. Non impostare inoltri automatici della posta di Ateneo su servizi di posta esterni (ad es. gmail, ...). Se il dispositivo non è dell'Università, prediligi l'uso della webmail.**

9. **Presta attenzione durante la navigazione in Internet evitando siti sconosciuti e rischiosi**

10. **Usa sistemi operativi e software aggiornati all'ultima versione disponibile evitando di installare programmi non più aggiornabili; non installare software provenienti da fonti non ufficiali, in particolare programmi, software o file che violino la licenza d'uso, illegali o modificati illegalmente**

11. **Utilizza delle password robuste (lunghe e complesse) e differenziate per i vari servizi creandone 1 per l'accesso al PC, 1 per i servizi di Unimi e tante password diverse quanti sono i servizi esterni che utilizzi**

12. **Come strumento per riunioni e meeting prediligi Microsoft Teams**

13. **Effettua sempre il log out dai Servizi/Portali di Ateneo**

14. **Usa sempre un atteggiamento cauto e prudente e non rivelare mai informazioni riservate**

15. **Se ritieni di aver subito un incidente informatico (allarme antivirus che segnali un software pericoloso; apertura erronea di allegati di una mail insidiosa) comunica l'accaduto con una mail a sicurezza@unimi.it - se nell'incidente sospetti una violazione di dati personali scrivi a violazione.dati@unimi.it.**

Premessa

Tutti i dipendenti dell'ente sono tenuti a seguire le indicazioni e le disposizioni dell'Università degli Studi di Milano in materia di sicurezza informatica e protezione dati personali, anche quando operano in modalità agile e ad agire in modo conforme alle normative vigenti.

Ai fini del presente documento, per risorse aziendali, si intende qualsiasi risorsa (dati, informazioni, dispositivi, sistemi, servizi) messa a disposizione del personale e/o dell'utente dall'Ateneo al fine di garantire i propri servizi e per rendere la propria attività lavorativa.

Si ricorda a tutto il personale che le risorse messe a disposizione per lo svolgimento delle regolari mansioni lavorative devono essere utilizzate solo ed esclusivamente a tale scopo. È vietata, quindi, qualsiasi attività che possa comportare un danno alle suddette risorse o che risulti in contrasto con il presente documento e/o, in generale, con la normativa vigente e con i regolamenti di Ateneo.

Ciascun dipendente è tenuto a mettere in atto, nell'ambito delle proprie attività di lavoro, tutte le misure di sicurezza ritenute idonee a scongiurare la possibilità di furti, frodi, accessi non autorizzati, danni, distruzioni o altri abusi nei confronti delle risorse d'Ateneo. Qualsiasi situazione anomala o sospetta, nonché eventuali furti, smarrimenti o danneggiamenti alle risorse aziendali deve essere prontamente segnalata al Settore Cybersecurity, Protezione Dati e Conformità della Direzione ICT attraverso il canale e-mail sicurezza@unimi.it.

In relazione al trattamento di dati personali, si ricorda che l'Università degli Studi di Milano, in qualità di titolare del trattamento dei dati personali dell'Ateneo, dispone che chiunque abbia accesso a dati personali, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, deve farlo in conformità al "Regolamento in materia di protezione dei dati personali dell'Università degli Studi di Milano", e secondo le modalità descritte nella **circolare rettorale 164/2019 del 30/10/2019 e nei suoi allegati che ne costituiscono parte integrante.** Le istruzioni dell'Ateneo per il trattamento dei dati personali sono reperibili nell'apposita sezione dedicata alla Sicurezza Informatica e alla Protezione dei dati, del portale work.unimi.it ai link qui di seguito riportati:

- Istruzioni per il trattamento dati
- Istruzioni per proteggersi dal phishing
- Istruzioni per la protezione da Data Breach

Tali istruzioni sono da considerarsi valide a tutti gli effetti anche nel caso la prestazione lavorativa sia resa in modalità agile.

In questo caso particolare devono essere prese ulteriori misure e cautele per la protezione delle informazioni trattate.

Indicazioni da seguire

Accesso sicuro alle risorse di Ateneo

Per svolgere l'attività lavorativa è richiesto l'utilizzo del servizio di VPN offerto dal Settore Cybersecurity, Protezione Dati e Conformità della Direzione ICT. Le informazioni per utilizzare il servizio sono disponibili al link Istruzioni VPN.

Dovrebbe apparire la l'icona che indica che la connessione è stata stabilita:

Si fa presente a tutti gli utenti che la VPN è ad uso esclusivo lavorativo, pertanto si invita a disconnettere la VPN dalla propria postazione di lavoro remota in caso di sospensione delle attività lavorative.

Per disconnettere la VPN è sufficiente posizionarsi sull'icona del Global Protect, e posizionarsi sulla rotellina dell'ingranaggio e cliccare su "**Disable**" come mostrato in figura.

Per ripristinare la VPN è sufficiente posizionarsi sull'icona del programma Global Protect, in basso a destra (Fig 1) e rappresentata da un mappamondo e cliccare su ENABLE (Fig 2). Dopo pochi secondi il sistema è già pronto ad operare in VPN.

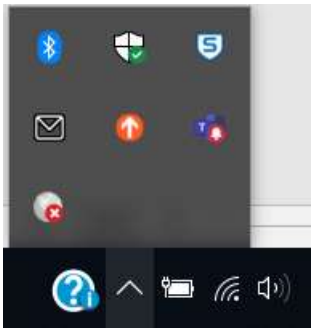


Figura 1

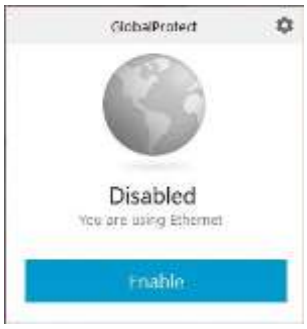


Figura 2

Connettività alla rete domestica

Il servizio VPN di Ateneo, descritto in precedenza, garantisce un alto livello di confidenzialità delle informazioni trasmesse in rete. E' buona norma essersi sincerati, quando ci si connette alla rete dati domestica, che sia stata modificata la password di default, impostata generalmente dal produttore del dispositivo, della connessione alla rete Wi-Fi di casa e la password di default di amministrazione del router Wi-Fi in quanto queste password potrebbero essere note ad altri o insicure.

Non connettersi mai per lavoro da hot spot pubblici come ad esempio aeroporti, stazioni, bar ecc. a meno che non sia attiva la VPN di Ateneo.

Accesso e Gestione del PC e dei dispositivi usati per il lavoro Agile

I dispositivi personali utilizzati per le attività lavorative devono essere usati con la massima diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro (Università o al proprio domicilio), avendo cura di adottare gli accorgimenti e le misure utili ad evitare il verificarsi di danni o sottrazioni di dati. A tal proposito occorre prestare particolare attenzione a non lasciare incustoditi i dispositivi portatili in auto, su treni o aerei.

I dispositivi devono essere integri non devono, cioè, essere stati sottoposti a operazioni che possano compromettere il corretto funzionamento dei meccanismi di protezione del software quali ad esempio jailbreaking e rooting dei dispositivi portatili o installazione di software non correttamente licenziato nei PC. È responsabilità degli utenti effettuare questa verifica.

L'accesso al portatile universitario deve avvenire attraverso un'utenza specifica, senza poteri di amministrazione del dispositivo, dedicata al lavoro agile e protetta da uno username e da una password che devono essere diverse dalle credenziali di Ateneo.

Stessa precauzione si può applicare sui dispositivi smartphone di tipo Android o iOS (telefoni, tablet, ..) dove è possibile attivare un apposito profilo di lavoro e separare in questo modo i dati privati da quelli legati ad esigenze lavorative. Istruzioni dettagliate su come creare il profilo di lavoro sono pubblicate sul sito di supporto di Android o Apple. Sincerarsi che l'accesso ai dispositivi sia sempre protetto da sistemi di autenticazione.

Deve essere anche previsto il salvaschermo (screensaver) con blocco automatico della sessione protetta da credenziali di autenticazione dopo al massimo 5 minuti di inattività.

È necessario che sulla postazione siano attivi sia il firewall personale che l'antivirus; questo significa che nell'angolo destro della barra delle applicazioni devono essere presenti le seguenti icone:

Per attivare il firewall di Windows seguire le seguenti istruzioni

Qualora l'antivirus non fosse installato si DEVE procedere alla sua installazione come di seguito spiegato.

Antivirus

Ogni pc usato per svolgere attività lavorative deve obbligatoriamente essere dotato del sistema antivirus di Ateneo, automaticamente e costantemente aggiornato. Le informazioni relative all'Antivirus di Ateneo sono reperibili sul portale di Ateneo alla pagina dedicata al servizio antivirus. E' importante garantire il corretto funzionamento e aggiornamento dell'antivirus di Ateneo.

Personal Firewall

La maggior parte dei sistemi operativi moderni è dotato di personal firewall, solitamente con una configurazione di default che permette un livello medio di sicurezza. È richiesto di non disabilitare mai il personal firewall o modificarne le impostazioni di default.

Dispositivi Esterni

Bisogna evitare di collegare al PC dispositivi mobili (penna USB, hard disk esterno o altri supporti esterni ecc.) poiché potrebbero veicolare virus o malware e potrebbero comportare la perdita di riservatezza, integrità e disponibilità delle informazioni.

E' sempre vietato collegare dispositivi mobili di cui non si conosce la provenienza.

Solo nel caso in cui si conosca la provenienza del dispositivo mobile e dovesse risultare assolutamente indispensabile il suo utilizzo, ne è consentito l'utilizzo in via eccezionale. In queste circostanze il dipendente dovrà effettuare preventivamente la scansione del dispositivo mobile con l'Antivirus di Ateneo.

Sui dispositivi mobili dovrà essere sempre adottata la cifratura e dovrà essere garantita la cancellazione tempestiva di quelli non necessari. Gli stessi dovranno essere custoditi con la massima diligenza.

Cifratura

Uno strumento chiave per garantire la riservatezza dei dati è la cifratura. Questa operazione risulta di fondamentale importanza quando i dati memorizzati sono dati *personali*, che sono memorizzati nell'HD del computer, su supporti removibili, o in cloud su sistemi centralizzati.

L'uso della cifratura è obbligatorio su tutti i dispositivi portatili, come notebook, USB pendrive e hard disk esterni. Le linee guide e il manuale sui diffusi sistemi di cifratura sono disponibili al seguente link.

Strumenti di Ateneo

I lavoratori nello svolgimento delle proprie attività, ~~Se~~ devono utilizzare sempre le soluzioni e gli strumenti di Ateneo che permettono di salvare i dati in remoto e garantiscono, in modo trasparente all'utente, la protezione e il backup dei dati. È importante non salvare i dati relativi al proprio lavoro in locale.

Il backup previene, quindi, la perdita di disponibilità dei dati. I sistemi centralizzati di Ateneo e i sistemi in cloud, normalmente, prevedono un backup automatico, senza alcuna interazione da parte degli utenti. Per maggiori informazioni sui backup centralizzati, contattare il referente tecnico di struttura.

A questo proposito gli utenti dell'Amministrazione Centrale possono accedere agli archivi presenti su Dataserver seguendo queste istruzioni. Gli utenti dei Dipartimenti possono utilizzare i file server o altre risorse eventualmente messe a disposizione all'interno della propria struttura. Tutti gli utenti dotati di credenziali @unimi.it possono condividere file e dati con altri soggetti autorizzati mediante il sistema di Ateneo Unimibox.

Posta elettronica

E' necessario prestare la massima attenzione nella gestione delle mail in arrivo nella propria casella di lavoro. Le email con particolari richieste o contenenti link sospetti devono essere trattate con la massima cautela. Alcune informazioni possono essere trovate nella Guida pratica per analizzare le email e Indicazioni utili a proteggersi dal Phishing pubblicate sul portale work.unimi.it nell'apposita sezione "Sicurezza informatica e protezione dei dati personali".

E' da privilegiare, nel caso il dispositivo in uso non sia fornito dall'Università o ove possibile, la gestione della posta elettronica di Ateneo tramite webmail in luogo dell'installazione, sul proprio dispositivo, di un programma di posta elettronica (ad esempio Outlook o Thunderbird); ciò consente di evitare di salvare la posta di lavoro sul proprio PC in quanto potrebbero esservi mail contenenti dati personali o informazioni riservate. Si ricorda inoltre che la casella di posta non deve essere utilizzata mai come archivio. Nel caso in cui si ricevano documenti contenenti dati

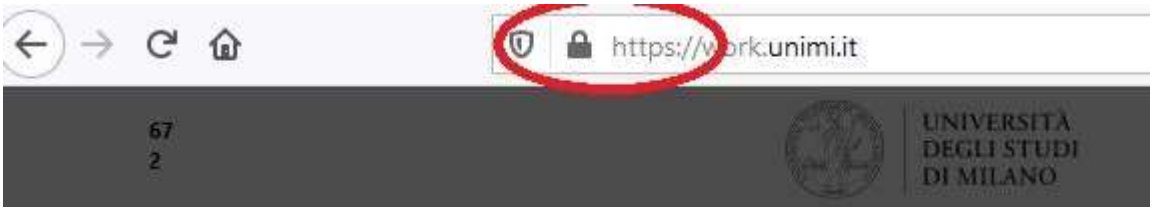
qualificabili come particolari[1] (ex sensibili) e di pertinenza dell'Ateneo, per il rispetto delle norme sulla protezione dei dati, si richiede di salvarli immediatamente negli spazi di archiviazione remota messi a disposizione dall'Ateneo e cancellarli dalla propria casella di posta elettronica.

Navigazione

Ciascun utente deve prestare molta attenzione alla navigazione, evitando di navigare in siti sconosciuti o potenzialmente rischiosi.

La navigazione deve comunque avvenire nel rispetto della legge, dell'ordine pubblico, del buon costume e delle norme di prudenza e cautela atte ad evitare infezioni del dispositivo e problemi di sicurezza al sistema informativo d'Ateneo e a evitare infezioni al dispositivo.

A tal proposito, a titolo puramente esemplificativo, è vietato: visitare siti che accolgono contenuti contrari alla morale e alle prescrizioni di legge; scaricare materiale elettronico tutelato dalle normative sul diritto d'Autore (software, file audio, file video, etc.); partecipare a forum non professionali e giochi in rete pubblica; utilizzare chat line, bacheche elettroniche e guest book non pertinenti ad esigenze lavorative o di studio. In generale, si consiglia di evitare di fornire propri dati personali a siti non sicuri: a tal proposito, è richiesto di controllare che il sito visitato utilizzi un protocollo di trasmissione dei dati di tipo **https://** visualizzabile nella barra dell'indirizzo sul browser come da immagine in allegato.



Software installato

Al fine di garantire un elevato livello di sicurezza del sistema operativo e degli applicativi installati sul pc e sui dispositivi mobili utilizzati per le attività lavorative, è indispensabile che gli stessi siano costantemente aggiornati e che siano applicate tempestivamente le patch di sicurezza appena disponibili.

Sul PC usato per il lavoro agile si raccomanda di non utilizzare mai software non aggiornati, con licenza scaduta o non più supportati dal fornitore. Devono essere installati SOLO programmi, o

[1] **Dato particolare:** i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

applicativi software regolarmente licenziati e non provenienti da supporti o siti non ufficiali, che potrebbero comportare l'installazione di programmi malevoli.

È vietato il download di software che non rispettino le caratteristiche sopra illustrate, software "pirata" e, in ogni caso, che non risultino strettamente necessari per le attività lavorative.

Politica di gestione password

Le password utilizzate per il lavoro agile come per ogni altra attività devono essere robuste ovvero con lunghezza idonea di almeno 12 caratteri, formate da lettere maiuscole e minuscole, numeri e/o caratteri e sempre diverse da quelle utilizzate in precedenza.

È opportuno che ogni utente disponga di password che devono essere diverse per ogni servizio utilizzato in particolare:

1. una password per accedere alla postazione di lavoro;
2. una password per accedere ai servizi di UNIMI utili allo svolgimento del lavoro agile;
3. altre password personali per svolgere attività non istituzionali.

Le credenziali d'autenticazione ai servizi e dispositivi d'Ateneo non devono essere rivelate a nessuno, né via mail, né a voce, né con altre modalità.

È importante non salvare le password sul browser e si ricorda, inoltre, che le credenziali utilizzate per lo svolgimento di attività lavorative non possono assolutamente essere comunicate o condivise con terzi, ivi compresi i colleghi. E' necessario assicurarsi di aver eseguito il log-out al termine di ciascuna attività.

Poiché l'uso di numerose password risulta spesso di difficile gestione è consigliato l'uso di un password manager che consente la memorizzazione e la gestione sicura di password multiple. I password manager sono programmi o app che archiviano in modo sicuro e cifrato le credenziali (username e password) di accesso ai servizi web e non solo, in una sorta di cassaforte ("Vault") virtuale, rendendola disponibile all'utente quando ne avrà bisogno. Sono protetti da una Master Password, che serve per aprirli e diventa perciò l'unica password che occorre ricordare inoltre hanno la capacità di generare automaticamente password sicure e complesse.

Un esempio di questo tipo di strumento, libero e disponibile per le piattaforme più diffuse, è KeePass

Strumenti per meeting e riunioni

Per le riunioni a distanza, l'Ateneo mette a disposizione Microsoft Teams come strumento di collaborazione istituzionale.

Log out (disconnessione) dai servizi/portali e dispositivi di Ateneo

In caso di assenza momentanea dalla propria postazione, ci si deve accertare che la sessione di lavoro non sia accessibile a terzi, facendo il log out dalla sessione o attivando il salvaschermo.

Dopo aver utilizzato i servizi ed i portali di Ateneo ed in generale tutti i servizi che richiedono l'autenticazione iniziale è sempre buona norma effettuare il log out cliccando sul tasto apposito: questo per evitare attacchi informatici che sfruttano le autenticazioni sui servizi ancora attivi.

Alla fine dell'attività lavorativa è richiesto il log out da tutti gli applicativi e lo spegnimento del pc che deve essere custodito in luogo sicuro. Stessa precauzione vale per i documenti cartacei contenenti informazioni riservate.

Comportamenti da adottare

Ciascun dipendente è tenuto ad osservare un atteggiamento quanto più cauto e prudente, al fine di preservare la sicurezza del sistema informativo universitario e delle informazioni dell'ente.

I dispositivi utilizzati per le attività lavorative devono essere usati con la massima diligenza, avendo cura di adottare gli accorgimenti e le misure utili ad evitare la manomissione involontaria e/o la sottrazione di dati.

Non bisogna mai rivelare informazioni confidenziali e riservate a persone non autorizzate, prestando attenzione anche a quelle situazioni in cui soggetti terzi potrebbero involontariamente venire a conoscenza delle suddette informazioni (ad esempio a causa della condivisione in spazi in cui si effettuano telefonate o si lavora al pc).

E' richiesto a ciascun dipendente di mantenere sempre un atteggiamento circospetto verso chiunque richieda informazioni confidenziali (ivi comprendendo dati personali o "sensibili") attraverso qualsivoglia mezzo. E' richiesto di non fornire informazioni private a terzi per telefono o email, senza essersi accertati dell'identità dell'utente e non rispondere alle mail sospette. Nel caso di dubbio, si può contattare telefonicamente la struttura o l'utente da cui sembra provenire il messaggio e chiedere chiarimenti.

Al fine di ridurre ulteriormente il rischio di compromettere la riservatezza, l'integrità e la disponibilità delle informazioni trattate mediante le risorse aziendali, si richiede a ciascun utente di assumere un atteggiamento collaborativo, che preveda la segnalazione, come illustrato al paragrafo successivo, di qualsiasi evento anomalo o dubbio, potenzialmente in grado di compromettere la sicurezza delle informazioni.

Cosa fare in caso di problemi di sicurezza informatica o di sospetta violazione dati

Il dipendente che operando da remoto riscontri problemi di sicurezza informatica, quali una segnalazione dell'antivirus, apra erroneamente un allegato di un messaggio di posta elettronica di dubbia provenienza, subisca un furto o smarrisca il proprio dispositivo ecc. è tenuto ad avvisare il Settore Cybersecurity, Protezione Dati e Conformità inviando immediatamente una email a **sicurezza@unimi.it** .

Nel caso di sospetto o certezza di violazione di dati personali, ad esempio a seguito dello smarrimento o furto del dispositivo o del pc, è necessario segnalare immediatamente l'accaduto al Settore Cybersecurity, Protezione Dati e Conformità e al Responsabile della Protezione Dati di Ateneo inviando una mail a **violazione.dati@unimi.it** secondo queste istruzioni

Riferimenti e approfondimenti

Per gli approfondimenti e gli aggiornamenti di quanto descritto nel presente documento, per le modalità di implementazione delle misure di sicurezza richieste e per la consultazione del materiale divulgativo in tema di protezione dei dati personali e sicurezza informatica, è possibile fare riferimento ai documenti del Settore "Cybersecurity, Protezione Dati e Conformità" di Ateneo pubblicati sul portale nella sezione dedicata alla "Sicurezza informatica e protezione dei dati personali" e in particolare:

Sicurezza Informatica e Protezione dei Dati Personali

Regolamenti Istruzioni e Linee Guida

Avvisi di Sicurezza