Requisiti tecnologici minimi per il lavoro remoto

L'attività di lavoro remoto da parte dei dipendenti dell'Ateneo necessita l'utilizzo di strumenti informatici che devono essere in dotazione al dipendente. In questo documento si effettua una disamina degli strumenti generalmente necessari anche se un'analisi più dettagliata per le singole posizioni va fatta dal capo ufficio prima di autorizzare il lavoro remoto.
In generale si possono individuare tre possibili modalità' di espletamento delle attività in telelavoro.

1. Attività di ufficio standard

Per le attività normali d'ufficio il dipendente potrà usare:

- Accesso alla posta elettronica personale e di ufficio https://webmail.unive.it
- Utilizzo on line degli applicativi Cineca tramite il browser web
- Utilizzo degli applicativi Sebina (biblioteche) tramite Browser web
- Accesso a Google Suite (Google Drive, Apps etc.)
- Utilizzo degli applicativi web oriented di Ateneo anche in area riservata

Per questo tipo di attività si consiglia:

1. Di preparare e salvare sul proprio Google Drive un documento che contenga i link ai sistemi web based utilizzati.
2. Assicurarsi di avere a disposizione sul PC che si intende utilizzare il pacchetto Microsoft Office 2013 o versioni superiori o pacchetti Open Source equivalenti (OpenOffice, LibreOffice etc.) o in alternativa predisporre l'accesso agli strumenti di office 365 messo a disposizione dall'Ateneo (www.office.com)
3. Assicurarsi di avere a disposizione una connessione ADSL o equivalente Banda >= 5 Mbps (in download)
4. Verificare che i documenti che si intende utilizzare siano a disposizione nello spazio Google Drive dell'ufficio.

Questa modalità è da considerarsi come standard e preferibile rispetto alle altre poichè richiede l'utilizzo di risorse hardware e software minimali.
Le riunioni di ufficio potranno essere effettuate con il sistema Google Meet e le comunicazioni rapide tra colleghi con Google Hangouts..
In particolare, si suggerisce un utilizzo esteso di Google Drive per ospitare dati e documenti di natura non critica sul piano di sicurezza e privacy, in quanto le politiche contrattuali definite dall'Ateneo con Google offrono sufficienti garanzie di sicurezza. Vantaggi offerti sono:

- Maggiore garanzia di accessibilità' in qualsiasi condizione di connessione alla rete,
- Facilità di condivisione e di gestione concorrente dei files
- Possibilità di accesso anche da piattaforme mobili (smartphone, tablet etc.)

Per l'accesso all'e-mail si sconsiglia l'utilizzo di client di posta (ad es. Thunderbird) a favore dell'accesso tramite browser.

2. Attività che richiedono necessariamente l'utilizzo di VPN

Il personale che abbia esigenze specifiche di utilizzo di alcune risorse come ad esempio:

- Editing Typo3 (sito Web)
- Aree condivise su fs.unive.it
- Accesso a postazioni VDI non Citrix (macchine virtuali Windows 7)
- Accesso RDP a PC di ufficio per chi utilizza una postazione hardware non virtuale
- Accesso a dispositivo di controllo in laboratori attrezzati
- Accesso a risorse di supercalcolo (DAIS)
- Accesso al sistema di ticketing (solo per il back office)

Dovrà accertarsi di avere a disposizione, oltre alle dotazioni di cui al punto 1, anche le seguenti dotazioni software:

1. Client Fortigate 6.0 (prelevabile all link www.unive.it/vpn , in cui sono riportate anche le relative istruzioni di installazione)

3. Attività' che richiedono l'utilizzo di Client Citrix (VDI)

Il personale che ha necessità di utilizzare specifici software installati sulla propria postazione VDI in uso presso l'Ateneo (es. Adobe Acrobat Pro, Client di Contabilità, Client Gestione Edifici etc.), dovrà avere a disposizione le dotazioni previste dal punto 1 a cui si aggiungono:

- PC con S.O. Windows 10 o MAC dotato di OSX 10.10 (Yosemite)
- Connessione ADSL o equivalente Banda >= 10 Mbps (in download) Client Citrix (https://www.unive.it/pag/38118/)

Per le modalità di accesso alla postazione VDI dall'esterno si faccia riferimento alle istruzioni riportate al link: https://www.unive.it/pag/38118/

Il terzo tipo di connessione è generalmente sconsigliato poichè qualora il numero degli utenti in telelavoro dovesse essere molto alto, il sistema VDI potrebbe manifestare dei problemi di carico. Di conseguenza, l'utilizzo delle workstation VDI da remoto deve essere limitato ai casi strettamente necessari e per il solo periodo di necessità. Ciò vale in particolare per l'utilizzo del disco Z per cui è consigliabile che i documenti da utilizzare durante il telelavoro siano conservati su un google drive di Area.

Tutti gli utenti che utilizzano i sistemi di lavoro remoto sono invitati , indipendentemente dalla modalità' scelta tra quelle descritte, ad abilitare il meccanismo di rinnovo password via SMS (www.unive.it/newpass). Questo meccanismo permetterà, in caso di scadenza della password, il rinnovo in autonomia delle credenziali. Il rinnovo delle credenziali al di fuori di questa procedura non potrà essere effettuato senza riconoscimento dell'utente in presenza.