LINEE GUIDA PER IL "LAVORO AGILE" IN SAPIENZA
Istruzioni operative e requisiti di sicurezza informatica

Il DPCM del 23.09.21 recante "*Disposizioni in materia di modalità ordinaria per lo svolgimento del lavoro nelle pubbliche amministrazioni*" (GU n.244 del 12.10.2021) ha stabilito che a decorrere dal 15.10.2021, la modalità ordinaria di svolgimento della prestazione lavorativa è quella svolta in presenza.
Sapienza ha recepito il DPCM con la circolare n. 89064 del 14.10.2021 e la circolare n. 84139 del 28.10.2021, che hanno disciplinato le nuove modalità di applicazione del lavoro agile in Sapienza (di seguito "LAS").
In particolare, sarà fornita dal Centro InfoSapienza al personale debitamente autorizzato in LAS, la strumentazione tecnologica necessaria per la prestazione lavorativa.
In base alle direttive nazionali sulla sicurezza informatica emanate dal governo e in linea con le misure minime di sicurezza ICT promosse da AGID, si rende necessario fornire opportuni requisiti di sicurezza a tutti i dipendenti in LAS al fine di fornire misure di tecniche ed organizzative per la protezione dei dati e delle informazioni trattate.

Di seguito le linee guida per illustrare agli utenti le modalità di accesso alla rete e ai servizi con particolare riguardo agli aspetti di sicurezza informatica e protezione di dati, distinte per tipologia di fornitura:

- **Linee guida per il personale dell'amministrazione centrale in LAS;**
- **Linee guida per il personale in LAS con pc di proprietà della struttura.**

LINEE GUIDA PER IL PERSONALE DELL'AMMINISTRAZIONE CENTRALE IN LAS

La dotazione fornita al personale dell'Amministrazione Centrale dal Centro InfoSapienza comprende:

- Computer portatile opportunamente configurato per l'accesso automatico alla rete WI-FI e alla VPN, abilitato all'autenticazione utente con le proprie credenziali (matricola e password) al fine di garantire la raggiungibilità dei servizi interni dell'Ateneo e di mantenere adeguati livelli di protezione in linea con le misure di sicurezza informatica adottate dall'Ateneo.
- Router 4G WI-FI (detto anche "saponetta") comprensivo di SIM dati (100GB mese) per la connettività ad Internet.

Postazione di lavoro

Per l'utilizzo corretto e sicuro della postazione di lavoro è fortemente raccomandato:

1. Utilizzare il dispositivo ad uso esclusivo della attività lavorativa;
2. Non memorizzare password e credenziali di accesso sugli applicativi, in particolare sul browser (Internet Explorer, Chrome, Firefox, Safari, Edge, etc);
3. Non collegare alla propria postazione periferiche esterne (pen-drive, hdd-esterno, etc) di cui non si è certi della provenienza. Effettuare prima di ogni utilizzo la scansione con l'antivirus;
4. Effettuare il logout dai servizi/portali della Sapienza utilizzati alla conclusione della prestazione lavorativa;
5. Attivare sul PC, laddove possibile, la funzionalità di cifratura dei supporti di memorizzazione (dischi fissi o mobili) al fine di garantire la riservatezza dei dati trattati in caso di furto o smarrimento;
6. Evitare, durante l'attività lavorativa, la navigazione web verso siti non necessari allo svolgimento delle attività istituzionali;

7. Non memorizzare documenti contenenti dati personali all'interno del dispositivo e preferire gli ambienti cloud istituzionali (Google Drive, OneDrive) o le cartelle condivise interne alla rete Sapienza;
8. Disattivare sul dispositivo, durante la prestazione in LAS, quando non necessario ogni servizio di connessione come WI-FI o Bluetooth.

Connettività Internet

La Sapienza mette a disposizione a tutto il personale in LAS un router 4G WI-FI (detto anche "saponetta") per la connessione ad Internet dotato di SIM con un traffico dati di 100Gb/mese così da permettere la connessione WI-FI al computer.

Di seguito si raccomanda di:

1) Utilizzare il router 4G come mezzo di connessione alla rete durante la prestazione lavorativa in LAS, lo stesso non può in nessun modo essere ceduto a terzi;
2) Non collegare al dispositivo mobile ulteriori dispositivi, come smartphone, tablet, computer, anche se considerati sicuri;
3) Non lasciare incustodito il dispositivo;
4) Non usare la funzione WPS del router 4G.

Accesso ai servizi Sapienza

Di seguito le indicazioni fortemente raccomandate per l'accesso ai servizi:

1) Accedere alla postazione di lavoro ordinaria in ufficio attraverso il protocollo *Remote Desktop Protocol* (RDP). Tale modalità consente la visualizzazione dello schermo e, quindi, di avere a disposizione tutti i servizi della postazione ordinaria e gli stessi livelli di sicurezza adottati dall'Ateneo;
2) Utilizzare per le riunioni in videoconferenza solo i servizi messi a disposizione dalla Struttura o da Sapienza (es. Meet e Zoom);
3) Evitare di aprire allegati sospetti, presenti nella propria casella di posta elettronica, provenienti da mittenti sconosciuti o esterni all'organizzazione;

4) Diffidare delle mail che chiedono di fornire credenziali di accesso, pin o informazioni riservate. Nessun servizio di Sapienza invia mail ai propri utenti con la richiesta di fornire o cambiare le credenziali di accesso ai sistemi.

LINEE GUIDA PER IL PERSONALE IN LAS CON PC DI PROPRIETÀ DELLA STRUTTURA.

Il personale afferente alle Strutture sarà fornito di router 4G WI-FI per la connettività Internet

Postazione di lavoro

Per l'utilizzo corretto e sicuro della postazione di lavoro è fortemente raccomandato:

1. Utilizzare il dispositivo ad uso esclusivo della attività lavorativa;
2. Disporre, in caso di condivisione del dispositivo tra più persone, di un proprio account dedicato;
3. Utilizzare sistemi operativi con licenza d'uso e pienamente supportati dai produttori;
4. Mantenere il sistema operativo e i software installati continuamente aggiornati prevedendo di impostare, laddove previsto, la funzionalità di aggiornamento automatico;
5. Utilizzare un software antivirus impostando l'aggiornamento automatico. Per chi ne fosse sprovvisto, Sapienza mette a disposizione della comunità universitaria il software antivirus Bitdefender reperibile all'indirizzo https://campus3.uniroma1.it/;
6. Accedere alla postazione possibilmente con un account utente non amministratore opportunamente dedicato all'accesso in LAS;

7. Proteggere l'accesso dell'account di cui al 6) con una password possibilmente nel rispetto della Password Policy di Ateneo reperibile all'indirizzo https://web.uniroma1.it/infosapienza/sites/default/files/passwordpolicy.pdf;
8. Non memorizzare password e credenziali di accesso sugli applicativi, in particolare sul browser (Internet Explorer, Chrome, Firefox, Safari, Edge, ecc);
9. Utilizzare, laddove possibile, sistemi di autenticazione a due fattori (2FA);
10. Attivare un sistema firewall sul proprio dispositivo al fine di filtrare solo il traffico autorizzato;
11. Non utilizzare software e/o applicativi di cui non si disponga della licenza d'uso;
12. Impostare il blocco schermo, o configurare la modalità automatica temporizzata di blocco, quando ci si allontana dalla propria postazione di lavoro;
13. Non collegare alla propria postazione periferiche esterne (pen-drive, hdd-esterno, etc) di cui non si è certi della provenienza. Effettuare prima di ogni utilizzo la scansione con l'antivirus;
14. Effettuare il logout dai servizi/portali della Sapienza utilizzati alla conclusione della prestazione lavorativa;
15. Attivare sul PC, laddove possibile, la funzionalità di cifratura dei supporti di memorizzazione (dischi fissi o mobili) al fine di garantire la riservatezza dei dati trattati in caso di furto o smarrimento;
16. Evitare, durante l'attività lavorativa, la navigazione web verso siti non necessari allo svolgimento delle attività istituzionali;
17. Evitare di memorizzare documenti contenenti dati personali all'interno del dispositivo e di preferire gli ambienti cloud istituzionali (Google Drive, OneDrive) o le cartelle condivise interne alla rete Sapienza;
18. Effettuare backup periodici dei dati memorizzati nel proprio dispositivo;
19. Disattivare sul dispositivo, durante la prestazione in LAS, di ogni servizio non necessario (WI-FI, Bluetooth).

Connettività Internet

La Sapienza mette a disposizione a tutto il personale in LAS un router 4G WI-FI (detto anche “saponetta”) per la connessione ad Internet, dotato di SIM con un traffico dati di 100Gb/mese così da permettere la connessione Wi-Fi al computer.

Per il funzionamento del router 4G fare riferimento al manuale operativo presente all’interno della confezione e si consiglia:

- di modificare tutte le password predefinite;
- di non memorizzare il PIN della SIM all’interno del dispositivo;
- utilizzare il router 4G come mezzo di connessione alla rete durante la prestazione lavorativa in LAS, lo stesso non può in nessun modo essere ceduto a terzi;
- Non collegare al dispositivo mobile ulteriori dispositivi, come smartphone, tablet, computer, anche se considerati sicuri;
- Non lasciare incustodito il dispositivo;
- Non usare la funzione WPS del router 4G.

Accesso in VPN

Sapienza per favorire l’accesso alla propria rete e servizi ha predisposto il servizio di VPN di Ateneo. Per l’installazione e configurazione della VPN si rimanda al seguente link https://web.uniroma1.it/infosapienza/servizio-vpn-di-ateneo.

È raccomandato effettuare la disconnessione dal servizio VPN al termine della prestazione lavorativa in LAS.

Accesso ai servizi

Di seguito le indicazioni raccomandate per l’accesso ai servizi:

1) Accedere alla postazione di lavoro ordinaria in ufficio attraverso il protocollo *Remote Desktop Protocol* (RDP). Tale modalità consente la visualizzazione

dello schermo e, quindi, di avere a disposizione tutti i servizi della postazione ordinaria e gli stessi livelli di sicurezza adottati dall'Ateneo;

2) Utilizzare per le riunioni in videoconferenza solo i servizi messi a disposizione dalla Struttura o da Sapienza (es. Meet e Zoom);

3) Evitare di aprire allegati sospetti, presenti nella propria casella di posta elettronica, provenienti da mittenti sconosciuti o esterni all'organizzazione;

4) Diffidare delle mail che chiedono di fornire credenziali di accesso, pin o informazioni riservate. Nessun servizio di Sapienza invia mail ai propri utenti con la richiesta di fornire o cambiare le credenziali di accesso ai sistemi.

Riferimenti

[Circolare Lavoro Agile del 06/03/2020]
https://www.uniroma1.it/sites/default/files/field_file_allegati/circolare0020438.pdf

[Circolare Lavoro Agile del 14/10/2021]
https://www.uniroma1.it/sites/default/files/field_file_allegati/circolare_0084139.pdf

[Circolare Lavoro Agile del 28/10/2021]
https://www.uniroma1.it/sites/default/files/field_file_allegati/circolare_0089064_modalita_sottoscrizione_accordi_lavoro_agile-signed-signed.pdf

[Piattaforma Zoom]
https://web.uniroma1.it/infosapienza/zoom-meeting-la-comunit-accademica

[VPN di Ateneo]
https://web.uniroma1.it/infosapienza/servizio-vpn-di-ateneo

[Sapienza password policy]
https://web.uniroma1.it/infosapienza/sites/default/files/passwordpolicy.pdf

[AGID Circolare 1-2/2017 - Misure minime di sicurezza ICT]
https://www.gazzettaufficiale.it/eli/id/2017/04/04/17A02399/sg