Allegato 4

LINEE GUIDA PER IL "LAVORO IN MODALITÀ AGILE" IN SAPIENZA - Rev. 04/2024

Istruzioni operative e requisiti di sicurezza informatica

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 lavoro agile al fine di fornire misure 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:

a. Linee guida per il personale in lavoro agile con postazione di lavoro amministrata dal Centro Infosapienza.
b. Linee guida per il personale in lavoro agile con pc di proprietà della struttura.

LINEE GUIDA PER IL PERSONALE IN LAVORO AGILE CON POSTAZIONE AMMINISTRATA DAL CENTRO INFOSAPIENZA

La dotazione fornita dal Centro InfoSapienza al personale autorizzato al lavoro agile comprende:

- Computer portatile opportunamente configurato per l'accesso automatico alla VPN (e al WIFI nel caso della fornitura del router 4G), 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.
- Eventuale Router 4G WI-FI (detto anche "saponetta") comprensivo di SIM dati per la connettività ad Internet, solo nei casi particolari di necessità per esigenze di svolgimento del servizio agile in luoghi non serviti o serviti male dalla rete.

Postazione di lavoro

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

1. Utilizzare il portatile ad uso esclusivo dell'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 lavoro agile, quando non necessario, il servizio di connessione Bluetooth.

Connettività Internet tramite rete residenziale

Per l'utilizzo di una connessione di rete di tipo residenziale per l'accesso ad Internet in sicurezza occorre:

a) Verificare che l'accesso sia protetto da una password e che la stessa non sia quella di fabbrica fornita con il modem/router;
b) verificare che sia altresì protetto algoritmo di cifratura aggiornato agli standard in uso o recenti;
c) evitare di utilizzare WIFI o reti cablate di tipo pubbliche e/o di tipo Captive Portal. Si potrà comunque utilizzare il wifi Eduroam e, nelle sedi dell'Ateneo ove presente, anche il WIFI Sapienza; si potrà utilizzare inoltre anche la rete cablata nelle sedi dell'Ateneo.

Connettività Internet tramite router 4G ("saponetta")

Solo nei casi particolari di necessità per esigenze di svolgimento del servizio agile in luoghi non serviti o serviti male dalla rete, Sapienza mette a disposizione del personale un router 4G WIFI (detto anche "saponetta"), dotato di SIM abilitata al traffico dati per la connessione ad internet del computer tramite WIFI dedicato.

Di seguito si raccomanda di:

a) Utilizzare il router 4G come mezzo di connessione alla rete durante la prestazione lavorativa in lavoro agile, lo stesso non può in nessun modo essere ceduto a terzi;
b) non collegare al router 4G ulteriori dispositivi, come smartphone, tablet, computer, per non sovraccaricare la connettività del dispositivo e provocare disservizi al computer dato in dotazione;
c) non usare la funzione WPS del router 4G.

In tutti i casi, si raccomanda di non lasciare incustoditi i dispositivi dati in dotazione al lavoratore durante il loro uso e funzionamento.

Accesso ai servizi Sapienza

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

a) Accedere alla postazione di lavoro ordinaria in ufficio attraverso il protocollo Remote Desktop Protocol (RDP) sfruttando il collegamento VPN. 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;
b) utilizzare per le riunioni in videoconferenza solo i servizi messi a disposizione dalla Struttura o da Sapienza (es. Meet e Zoom);
c) evitare di aprire allegati sospetti, presenti nella propria casella di posta elettronica, provenienti da mittenti sconosciuti o esterni all'organizzazione;
d) 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 LAVORO AGILE CON PC DI PROPRIETÀ DELLA STRUTTURA.

In alternativa alla postazione di lavoro fornita e amministrata dal Centro Infosapienza, il personale afferente a Facoltà, Dipartimenti e Centri potrà utilizzare una postazione fornita dalla propria struttura.

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 lavoro agile;
7. Proteggere l'accesso dell'account di cui al 6) con una password nel rispetto della Password Policy di Ateneo *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 lavoro agile, quando non necessario, il servizio di connessione Bluetooth.

Connettività Internet tramite rete residenziale

Per l'utilizzo di una connessione di rete di tipo residenziale per l'accesso ad Internet in sicurezza occorre:

a) Verificare che l'accesso sia protetto da una password e che la stessa non sia quella di fabbrica fornita con il modem/router;
b) verificare che sia altresì protetto da un algoritmo di cifratura aggiornato agli standard in uso o recenti;
c) evitare di utilizzare WIFI o reti cablate di tipo pubbliche e/o di tipo Captive Portal. Si potrà comunque utilizzare il wifi Eduroam e, nelle sedi dell'Ateneo ove presente, anche il WIFI Sapienza; si potrà utilizzare inoltre anche la rete cablata nelle sedi dell'Ateneo.

Connettività Internet tramite router 4G ("saponetta")

Solo nei casi particolari di necessità per esigenze di svolgimento del servizio agile in luoghi non serviti o serviti male dalla rete, la Sapienza mette a disposizione del personale un router 4G WIFI (detto anche "saponetta"), dotato di SIM abilitata al traffico dati per la connessione ad internet del computer tramite WIFI dedicato.

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

a) di modificare tutte le password predefinite;
b) di non memorizzare il PIN della SIM all'interno del dispositivo;
c) utilizzare il router 4G come mezzo di connessione alla rete durante la prestazione lavorativa in lavoro agile, lo stesso non può in nessun modo essere ceduto a terzi;
d) Non collegare al router 4G ulteriori dispositivi, come smartphone, tablet, computer, per non sovraccaricare la connettività del dispositivo e provocare disservizi al computer dato in dotazione;
e) Non usare la funzione WPS del router 4G.

In tutti i casi, si raccomanda di non lasciare incustoditi i dispositivi dati in dotazione al lavoratore durante il loro uso e funzionamento.

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 lavoro agile.

Accesso ai servizi

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

a) Accedere alla postazione di lavoro ordinaria in ufficio attraverso il protocollo Remote Desktop Protocol (RDP) sfruttando il collegamento VPN. 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;
b) utilizzare per le riunioni in videoconferenza solo i servizi messi a disposizione dalla Struttura o da Sapienza (es. Meet e Zoom);
c) evitare di aprire allegati sospetti, presenti nella propria casella di posta elettronica, provenienti da mittenti sconosciuti o esterni all'organizzazione;
d) 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

[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

Contatti

Per eventuali necessità di assistenza sulla postazione di lavoro agile contattare l'Help-desk di Infosapienza: supportoDM@r1spa.it

Il/La Dipendente

_____

La Responsabile di Struttura

_____