

Modulo Allegato 3

ISTRUZIONI OPERATIVE PER LA PROTEZIONE DEI DATI PER I DIPENDENTI IN REGIME DI LAVORO AGILE:

VADEMECUM PER LAVORARE ONLINE IN SICUREZZA

Il presente documento contiene le istruzioni operative per i dipendenti di AREUS Sardegna in materia di privacy e protezione dei dati personali, da utilizzarsi nell'ambito dello svolgimento della prestazione lavorativa in modalità di lavoro agile, conformemente al Regolamento UE 2016/679 (GDPR), secondo le indicazioni contenute nella circolare AGID del 18/04/2017 (disposizioni in materia di sicurezza informatica) e al D.lgs. 196/2003, come modificato dal Decreto legislativo n.101/2018.

Sono individuate nell'informativa le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni.

Per risorse informatiche, si intende qualsiasi risorsa (dati, informazioni, dispositivi quali pc, portatili, telefoni aziendali, sistemi, servizi etc...) messa a disposizione dall'Azienda e/o in possesso del dipendente necessaria a garantire l'attività lavorativa in modalità agile.

Il dipendente è responsabile del corretto uso delle risorse informatiche con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali.

Al riguardo, si intende focalizzare l'attenzione sui seguenti accorgimenti per lavorare da remoto in modo sicuro:

- Utilizza le risorse rese disponibili messe dall'Azienda solo ed esclusivamente per lo svolgimento delle mansioni lavorative;
- Accertati di usare sempre la VPN fornita dall' Azienda;
- Configura una buona password sul router Wi-Fi di casa per prevenire facili intercettazioni del traffico;
- Tutti i computer, sia desktop che portatili, devono avere installato e attivo il software antivirus dell'Azienda o personale, con firewall attivato e devono essere mantenuti costantemente aggiornati con le patch di sicurezza del sistema operativo e degli applicativi utilizzati;
- Utilizza un profilo di accesso al pc dedicato al lavoro protetto da credenziali (Username e password) che siano sicure, non note ad altri e mai comunicate a terzi. In particolare, la password deve essere univoca (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente), cambiata frequentemente (almeno ogni 6 mesi) e regolarmente, e sempre diversa da quelle utilizzate in precedenza. Le password non devono essere mai scritte e conservate in luoghi e modi che non garantiscano adeguata protezione;
- Usa sistemi operativi e software aggiornati all'ultima versione disponibile. Non installare software provenienti da fonti non ufficiali, in particolare programmi, software o file che violino la licenza d'uso, illegali o modificati illegalmente;
- Imposta il blocco del personal computer automatico ("salvaschermo") quando ti allontani dalla postazione di lavoro;
- Non collegare dispositivi esterni (penna USB, Hard Disk esterni) di cui non conosci la provenienza. Per salvare e o condividere le informazioni utilizza sempre gli strumenti Aziendali che garantiscono maggior affidabilità oltre che il backup dei dati;
- Il trattamento dei dati deve essere improntato ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi;
- Presta attenzione durante la navigazione in Internet evitando siti sconosciuti e rischiosi;
- Quando leggi la posta elettronica, evita di scaricare allegati o cliccare su link ricevuti in e-mail da mittenti sconosciuti;
- Utilizza l'account di posta aziendale;

- Effettua sempre il log out dai Servizi/Portale Aziendali;
- Usa sempre un atteggiamento misurato e attento per evitare di rivelare involontariamente informazioni riservate;
- Prestare attenzione alla fuga di notizie ed in ogni caso avvertire il Titolare e il DPO per le notifiche necessarie;
- Se si ritiene di aver subito un incidente informatico (allarme antivirus che segnali un software pericoloso; apertura erronea di allegati di una mail insidiosa) deve essere comunicato l'accaduto con una mail ai sistemi informativi aziendali competenti (Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica, Sistemi Informativi Amministrativi e Sicurezza ICT);
- Partecipare alla formazione obbligatoria che sarà erogata in materia;
- La protezione dei dati si applica anche a documenti cartacei, cui va garantita custodia e controllo. Pertanto, la documentazione cartacea contenente dati personali e amministrativa in genere, deve essere custodita per evitare l'accesso agli stessi da parte di soggetti non autorizzati.

Ottempera agli obblighi a carico del lavoratore prescritti dal D. Lgs. 81/08 e ss.mm. ii. secondo la informazione e formazione ricevute.

Le istruzioni e/o raccomandazioni impartite sono da ritenersi, a tutti gli effetti, quali direttive provenienti dal proprio datore di lavoro e, in quanto tali, il loro mancato rispetto potrebbe generare delle responsabilità a carico del dipendente.

Data _____

Firma del Dipendente
