NORME GENERALI RELATIVE AL TRATTAMENTO DEI DATI PERSONALI

Documenti cartacei

1. I documenti cartacei contenenti dati personali, per evitare l'accesso agli stessi da parte di soggetti non autorizzati, devono essere custoditi in armadi chiusi a chiave
2. Occorre prestare attenzione alla stampa di documenti o alla ricezione di fax su stampanti condivise o fotocopiatrici di rete, avendo cura di recuperare tempestivamente la stampa e non lasciando i documenti incustoditi

Postazione di lavoro

1. La postazione di lavoro deve essere configurata in modo che sia impostato l'avvio automatico dello screensaver dopo al massimo 5 minuti di inattività del Personal Computer e, in caso di assenza momentanea dal proprio posto di lavoro, ci si deve accertare che la sessione di lavoro non sia accessibile a terzi, facendo logout o attivando il salvaschermo con blocco della sessione protetta da credenziali di autenticazione

Personal Computer

1. Tutti i PC (desktop e portatili), al termine delle ore di servizio, devono essere spenti
2. Tutti i PC (desktop e portatili), contenenti dati personali propri o di terzi, devono adottare meccanismi di cifratura dei dati presenti nella memoria di massa non volatile
3. Bisogna prestare particolare attenzione alla custodia di supporti esterni mobili (chiavette USB, dischi esterni, tablet, smartphone), evitando di lasciarli in luoghi non protetti

Credenziali di accesso

1. È obbligatorio impostare delle credenziali di accesso sicure, non note ad altri e mai comunicate a terzi. La password deve essere univoca, robusta, cambiata frequentemente e sempre diversa da quelle utilizzate in precedenza
2. Non bisogna usare la stessa password usata per l'accesso ai sistemi e servizi universitari per accedere ad applicazioni o siti che siano esterni al dominio Unimi
3. Le password non devono essere mai scritte e conservate in luoghi e modi che non garantiscano adeguata protezione
4. È vietato fornire o rendere disponibili a soggetti esterni all'Ateneo informazioni tecniche riferite alla rete e ai sistemi di Ateneo

Antivirus

1. Su tutti i computer deve essere installato ed attivo il software antivirus dell'Ateneo (Sophos)
2. Tutti i computer devono essere mantenuti costantemente aggiornati con le patch di sicurezza del sistema operativo e degli applicativi utilizzati

Backup

1. È obbligatorio adottare tutte le misure necessarie per salvaguardare i dati (e consentirne il ripristino) mediante regolari backup
2. La copia cifrata di backup dei dati deve essere custodita offline, cioè scollegata dal sistema che ospita i dati
3. È vietato utilizzare servizi di archiviazione e condivisione file offerti da operatori commerciali (ad es. Google Drive, Dropbox, iCloud) per backup di dati personali inerenti le attività istituzionali