Trattamenti CON ausilio di strumenti elettronici

Ogni persona autorizzata al trattamento dei dati personali deve utilizzare le **risorse informatiche** che le sono state assegnate in conformità al Regolamento per l'accesso ai servizi di rete dell'Università di Pisa e attenendosi alle indicazioni contenute nei seguenti paragrafi.

Gestione delle credenziali di Ateneo

Ogni persona autorizzata al trattamento dei dati personali con strumenti elettronici deve essere dotata di **credenziali di autenticazione** (qui di seguito denominate *Credenziali di Ateneo*), costituite da un codice di identificazione personale (*user-id*) associato ad una parola chiave riservata (*password*).

Per quanto riguarda la corretta gestione di quest'ultima, ciascun soggetto autorizzato al trattamento dei dati personali deve attenersi alle seguenti indicazioni.

- Impostare una password che abbia una lunghezza di **almeno 8 caratteri**, utilizzando lettere, cifre numeriche e simboli. Si sconsiglia fortemente di utilizzare sequenze ovvie di numeri o lo stesso numero ripetuto più volte o di basare la propria password informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il proprio codice fiscale.
- Cambiare la propria password al primo accesso e, successivamente, con cadenza almeno **semestrale**.
- **Non trascrivere** la propria password su supporti facilmente accessibili a terzi (fogli, post-it, ecc.).
- **Non salvare** la propria password in programmi come browser (Chrome, Edge, Firefox, ecc.) o client di posta elettronica (Outlook, Thunderbird, ecc.) installati sul proprio pc o su pc di altri utenti.
- Mantenere la propria password **riservata**, evitando in ogni caso di condividerla con terzi, anche se autorizzati al trattamento.
- **Sostituire immediatamente** la propria password nel caso in cui si sospetti che questa sia in possesso di terzi.

Gestione dei dispositivi

Ogni persona autorizzata al trattamento dei dati personali con strumenti elettronici deve attenersi alle seguenti regole relative alla gestione dei dispositivi di memorizzazione ed elaborazione dati (qui di seguito denominati *dispositivi)* quali pc, smartphone, tablet, ecc., sia di **proprietà dell'Ateneo** che **personali**, nel caso in cui quest'ultimi vengano utilizzati nell'ambito della prioria attività lavorativa.

- L'accesso ai dispositivi deve in ogni caso essere **protetto** da password o da altra tecnologia che permetta di identificare l'utente in modo univoco (impronta digitale, segno di sblocco, codice, ecc.).
- Una volta eseguito l'accesso ad un dispositivo, è necessario procedere al suo **blocco** ogniqualvolta sia necessario lasciarlo incustodito, in modo che sia necessario eseguire di nuovo l'accesso prima del successivo utilizzo.
- Per evitare consultazioni illecite, deve sempre essere attivato il salvaschermo.
- I dati personali presenti sui dispositivi locali in unica copia devono essere **salvati**, con cadenza almeno settimanale, **sul servizio cloud** di Ateneo (OneDrive) utilizzando l'utente collegato alle proprie credenziali di Ateneo, o su supporto elettronico removibile (penna USB, ecc.). In caso di salvataggio su supporto elettronico removibile, tale supporto deve essere conservate in **armadi o cassetti chiusi a chiave** o in stanze ad accesso limitato**.**

- In caso di ricezione di messaggi di posta elettronica, è necessario assicurarsi dell'**origine dei messaggi** prima di aprire link o file allegati in essi contenuti, al fine di ridurre al minimo il rischio di attacco da parte di software malevolo.

Gestione dei dispositivi NON gestiti dal personale tecnico

Le persone autorizzate al trattamento dei dati che utilizzino dispositivi **NON gestiti dal personale tecnico informatico** della Direzione Servizi Informatici e statistici (qui di seguito denominati *personale tecnico*) devono attenersi, oltre che alle indicazioni presenti nel paragrafo **Gestione dei dispositivi,** anche alle seguenti indicazioni.

- Nel caso in cui un dispositivo o un supporto elettronico removibile, NON gestito dal personale tecnico, utilizzato per trattare dati personali, venga **destinato a diverso uso**, è necessario garantire che le informazioni in esso precedentemente contenute non siano in alcun modo intelligibili e ricostruibili tecnicamente.
- Coloro che utilizzano per il trattamento dei dati dispositivi NON gestiti dal personale tecnico, devono garantirne l'**aggiornamento almeno semestrale** del sistema operativo e dei software necessari per il rilevamento e la gestione di software malevolo (antivirus, ecc.) qualora questo non comprometta la funzionalità del dispositivo in uso. Laddove l'aggiornamento non risulti possibile senza compromettere la funzionalità del dispositivo in uso, è necessario darne **tempestiva comunicazione** al Responsabile per la sicurezza informatica e al Responsabile per la transizione al digitale.
- Nel caso in cui coloro che utilizzano per il trattamento dei dati dispositivi NON gestiti dal personale tecnico abbiano l'esigenza di installare applicativi software su tali dispositivi, devono assicurarsi di essere in possesso della **licenza necessaria** e che l'installazione dell'applicativo non comprometta l'**integrità** dei dispositivi stessi. In caso di dubbio è necessario rivolgersi al personale tecnico.

In caso di dispositivi gestiti dal personale tecnico, le indicazioni fornite in questo paragrafo saranno di competenza dello stesso personale tecnico.

Uso corretto di Internet

- Evitare di scaricare dalla rete file e software di uso non direttamente riferibili all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete d'Ateneo. I software necessari all'attività lavorativa devono essere richiesti alle competenti strutture universitarie.
- Usare Internet solo per svolgere l'attività lavorativa; i siti web spesso nascondono insidie per i visitatori meno esperti.

Uso corretto della posta elettronica

- Quando si renda necessario inviare la stessa comunicazione a più destinatari e il contenuto della comunicazione sia strettamente personale o contenga categorie di dati che necessitano un trattamento particolare, per esempio dati di salute, inviare la comunicazione per email a ciascun destinatario separatamente, oppure utilizzare lo strumento della copia conoscenza nascosta (CCN) per rendere ogni indirizzo riservato.
- Non leggere le caselle personali non istituzionali via webmail, in quanto alcuni provider esterni non proteggono dai virus.