La protezione dei dati personali
Attuazione del D. Lgs. 196/2003

MANUALE AD USO DEI RESPONSABILI E DEGLI INCARICATI

Versione: 2
Numero totale pagine: 19

ELENCO DEI CONTENUTI

MANUALE AD USO DEI RESPONSABILI E DEGLI INCARICATI

1 MISURE MINIME DI SICUREZZA

1.1 Premessa

Le **"misure minime"** sono costituite da quel complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali che l'Ateneo è tenuto ad adottare per ridurre al minimo i rischi di distruzione o di perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e che configurano il livello minimo di protezione richiesto dal Decreto Legislativo 196/2003 in materia di protezione dei dati personali.

Poiché il trattamento di dati personali può essere effettuato sia attraverso sistemi automatizzati sia attraverso supporti cartacei, è necessario distinguere tra:

1) Trattamenti automatizzati (effettuati con strumenti informatici e telematici)
2) Trattamenti non automatizzati (cartacei).

E' opportuno ricordare che, in tutti i casi, il trattamento dei dati personali da parte di ciascun Incaricato va preventivamente autorizzato dal rispettivo Responsabile e che l'autorizzazione al trattamento di dati personali deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento proprie della struttura.

Nel caso in cui vengano gestiti dati **personali**, il Responsabile del trattamento dei dati dovrà autorizzare per iscritto gli Incaricati ed assegnare loro il relativo ambito di trattamento coerente con quanto riportato nell'ultima versione pubblicata della tabella Ambiti_Trattamento, procedendo alla revoca della detta autorizzazione in tutti i casi di perdita della qualità che consente all'incaricato l'accesso ai dati personali (per es.: per trasferimento del dipendente ad altro ufficio, per assegnazione ad altre attività, per estinzione del rapporto di lavoro con l'Ateneo).

Per il conferimento e la revoca dell'incarico, il Responsabile dovrà utilizzare il modello SICURDAT opportuno, relativo alla tipologia di trattamento effettuato su cui dovrà essere apposta anche la firma degli Incaricati al trattamento per attestare l'avvenuta comunicazione dell'incarico a lui affidato e dell'ambito di trattamento che gli è consentito. Tali modelli, con la conferma degli incarichi dovranno comunque essere inviati alla Direzione Amministrativa entro il **30 GENNAIO** di ciascun anno, insieme con il "Questionario sullo stato di attuazione della normativa in materia di tutela della privacy" fornito.

1.2 Trattamenti automatizzati

Nell'ambito di tali trattamenti è necessario distinguere tra:

a) PC **non** collegati in rete;
b) PC collegati in rete ma **non** utilizzanti applicazioni informatiche centralizzate;
c) PC collegati in rete ed utilizzanti le applicazioni informatiche centralizzate.

1.2.1 Adempimenti di carattere generale previsti per tutti i PC

Tutti i PC devono essere accessibili attraverso l'utilizzo di un sistema di autorizzazione che preceda qualunque interazione con il sistema, mediante l'utilizzo di password da inserire all'atto dell'accensione della macchina. La password di accensione può essere di BIOS oppure, se il PC è inserito in un dominio, di rete e deve comunque essere di lunghezza non inferiore a 8 caratteri o del massimo numero di caratteri consentiti dal sistema.

La password BIOS deve essere modificabile dall'Incaricato e variata almeno ogni sei mesi. Nel caso in cui sul PC risiedano dati sensibili o giudiziari, tale password deve essere modificata almeno ogni tre mesi.

Le credenziali per l'autenticazione al dominio di rete (nel caso dei PC di tipo b) o c)) sono richieste mediante il modulo SICURDAT/B. Coerentemente con quanto prescritto dal Disciplinare Tecnico allegato al D.Lgs. 196/2003, la password di rete scade automaticamente ogni tre mesi e deve essere modificata dall'Incaricato. Qualora, scaduto tale termine, la password non è modificata per ulteriori sei mesi, le credenziali sono disattivate. L'istanza di riattivazione va presentata, a cura del Responsabile, mediante il modello SICURDAT/B. Infine, dopo cinque tentativi di connessione falliti, il codice identificativo (userid) è disabilitato. La richiesta di riabilitazione è effettuata dall'Incaricato mediante Help Desk (al numero 76799) del Centro Servizi Informatici d'Ateneo (CSI).

In sintesi, le regole valide per l'utilizzo delle credenziali di autenticazione:

Tabella 1 – Regole valide per l'utilizzo della password di BIOS

DESCRIZIONE	REGOLA
La password di BIOS può essere modificata dall'utente?	SI
Quale è la durata della password di BIOS?	6 mesi oppure 3 mesi nel caso di trattamenti con dati sensibili o giudiziari
La password viene revocata in caso di mancato utilizzo?	NO
La password ha una lunghezza minima?	SI, 6 caratteri o comunque del massimo numero di caratteri consentiti dal BIOS del PC

Tabella 2 – Regole valide per userid e password per l'accesso alla rete

DESCRIZIONE	REGOLA
La password di rete può essere modificata dall'utente?	SI
Quale è la durata della password di rete?	3 mesi
Lo userid viene revocato in caso di mancato utilizzo?	SI, dopo sei mesi a partire dall'ultimo rinnovo password non eseguito
La password di rete ha una lunghezza minima?	SI, 8 caratteri
Quanti sono i tentativi di prova di una password di rete prima che lo USERID sia disabilitato?	5

La password di accensione è personale per cui l'Incaricato che utilizza l'elaboratore deve essere il solo a conoscerla e deve conseguentemente custodirla con cura affinché non venga accidentalmente diffusa.

Si sottolinea che l'attenta custodia della password di accensione va effettuata anche nell'interesse dello stesso utente al fine di non esporsi a dover rispondere di attività svolte da altri soggetti tramite il PC a lui assegnato.

Al fine di consentire l'uso del PC anche in caso di impedimento dell'Incaricato che lo utilizza normalmente, questi dovrà consegnare al Responsabile del trattamento dei dati della struttura una busta chiusa contenente la propria password e provvedere a sostituirla in occasione dell'adozione di una nuova password.

Il Responsabile del trattamento dei dati, in caso di impedimento temporaneo di un dipendente, qualora sia indispensabile utilizzare il PC a questi assegnato (anche per effettuare un intervento tecnico di manutenzione da parte del personale autorizzato), aprirà la busta contenente la relativa password e la fornirà ad altro dipendente per consentirgli l'utilizzo del detto PC. La busta, con l'indicazione della data della sua apertura, dovrà essere conservata a cura del Responsabile fino alla consegna della busta contenente la nuova password da parte del dipendente che è stato temporaneamente impedito.

Il Responsabile è tenuto, inoltre, a verificare la corretta applicazione delle disposizioni relative alla password di accensione del PC, riscontrando in particolare la sostituzione, ogni tre mesi, delle password (vale a dire delle buste contenenti le stesse).

Coerentemente con quanto specificato al paragrafo 2.5 del presente documento, tutti i PC devono essere protetti dagli effetti di virus informatici mediante opportuno programma antivirus. Al fine di ridurre l'insorgere di problemi correlati a virus informatici, si rimanda al sopra citato paragrafo.

Il Responsabile e gli Incaricati si attengono alle istruzioni di seguito riportate.

Il programma antivirus, per i PC collegati in rete, deve essere aggiornato, o automaticamente o su richiesta dell'utente, con cadenza almeno settimanale. Per i PC non collegati in rete l'aggiornamento del programma antivirus deve essere effettuato con cadenza almeno mensile.

Il Responsabile del trattamento dei dati della struttura è tenuto a verificare la corretta applicazione delle presenti disposizioni, accertando che tutti i PC dell'Ufficio siano dotati del programma antivirus. Nel caso riscontri la mancanza di tali protezioni minime, il Responsabile è tenuto a darne immediata segnalazione al Centro Servizi Informativi d'Ateneo (CSI) mediante Help Desk (al numero 76799), in modo tale da far attivare il necessario intervento tecnico.

Nel caso in cui da parte del programma antivirus sia riscontrata la presenza di un virus informatico sul PC, l'Incaricato segue le istruzioni riportate sullo schermo dal programma ed avverte contestualmente il Responsabile del trattamento dei dati dell'evento. Quest'ultimo, dopo aver verificato che siano state rispettate le misure minime di protezione da virus informatici, provvede a segnalare allo CSI, tramite help desk, l'evento per eventuali e successivi interventi tecnici.

1.2.2 Adempimenti specifici previsti per il caso a)

In questo caso, deve essere obbligatoriamente utilizzata la password BIOS.

Per quanto riguarda la disponibilità dei dati personali trattati con PC non collegati in rete, il Responsabile è tenuto a verificare che, con cadenza almeno settimanale, tali dati siano archiviati su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) e che tali supporti siano conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 1.3.

1.2.3 Adempimenti specifici previsti per il caso b)

Tutti i PC collegati in rete devono, obbligatoriamente, essere collegati ad un server di dominio per il controllo di autorizzazione. A ciascun Incaricato è in tal caso assegnato un codice identificativo personale ed una password di rete mediante i quali l'Incaricato può accedere ed utilizzare le risorse di rete. Ciascun Incaricato in possesso di una credenziale di autenticazione alla rete ha accesso, in lettura e scrittura, ad una cartella dedicata al proprio Ufficio e ad una cartella personale, entrambe di capacità pari a 100 MB. Richieste di accessibilità ad ulteriori risorse di rete sono specificate ed autorizzate mediante il modulo SICURDAT/B.

L'utilizzo della autenticazione tramite il server di dominio non esclude l'utilizzo della password BIOS.

Per quanto riguarda la disponibilità dei dati personali trattati con PC collegati in rete, il Responsabile è tenuto a verificare che, con cadenza almeno settimanale, tali dati siano archiviati sul server di dominio, nelle cartelle di lavoro messe a disposizione di ciascun Incaricato. In casi eccezionali, il salvataggio dei dati può essere effettuato su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) che devono essere conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 1.3.

1.2.4 Adempimenti specifici previsti per il caso c)

A tali PC si applicano le norme previste per il caso b), con l'aggiunta delle prescrizioni di seguito riportate.

Ad ogni utente delle applicazioni informatiche centralizzate, per ciascuna applicazione, sono associati un codice identificativo personale, una password ed eventualmente un profilo di abilitazione.

Il Responsabile del trattamento dei dati dovrà individuare tassativamente per iscritto, compilando l'apposito modello SICURDAT/B, gli Incaricati dei trattamenti informatizzati mediante procedure centralizzate. Tale incarico rappresenta, implicitamente, l'autorizzazione all'utilizzo della corrispondente procedura informatica. I permessi dell'utente saranno tali da consentire le operazioni di trattamento richieste nel modello SICURDAT/B.

Di seguito, infine, si riportano alcune informazioni utili sulla gestione del codice identificativo personale (userid) e della password per l'accesso alle applicazioni informatiche centralizzate.

Ad ogni utente delle applicazioni informatiche centralizzate è associato un codice identificativo personale (userid), una password ed un profilo di abilitazione. Alcune applicazioni prevedono due diversi livelli di identificazione: uno di *sistema* ed uno *applicativo*. Le applicazioni informatiche riportate nel mod. SICURDAT/B che prevedono un doppio livello di identificazione sono: la procedura di Rilevazione Presenze (PRES), la procedura Finanziaria (FINUNI), la procedura Fiscale (FISC) e la procedura Gestione Ticket (GTIK). Per queste procedure, l'utente deve identificarsi preliminarmente verso il *sistema*, attraverso la maschera di collegamento al CSI e, successivamente, identificarsi verso *l'applicazione* che intende utilizzare.

Le altre applicazioni informatiche prevedono un solo livello di identificazione dell'utente. Queste ultime sono: la procedura di Gestione del Personale (ASIP), la procedura Segreteria Studenti (GEDAS), la procedura Organi Collegiali (SIOC), la procedura Protocollo (SIPR), la procedura di Gestione dei Dottorati di Ricerca (ASIB), la procedura di valutazione comparativa (VALCOM), la procedura per la gestione delle utenze e del traffico telefonico (GUTTEL).

A seconda del tipo di applicazione informatica utilizzata, le regole applicabili allo userid e alla password, sono diverse. In particolare il quadro delle regole attualmente in essere, è riportato nella Tabella 3.

Tabella 3 – Regole valide per userid e password delle applicazioni informatiche centralizzate

	ASIB	ASIP	GEDAS	SIOC/SIPR	GUTTEL	FINUNI	FISC	GTIK	SIRP	VALCOM	INPDAP
Livelli di identificazione	1	1	1	1	2	2	2	2	2	1	2
La password può essere modificata dall'utente?	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	NO
Quale è la durata della password ?		30 gg.	30 gg.		6 mesi	30 gg.	30 gg.	30 gg.	30 gg.	60gg.	
Lo userid viene revocato in caso di mancato utilizzo?		SI, dopo 45 gg.				SI, dopo 45 gg.	SI, dopo 45 gg.	SI, dopo 45 gg.			
La password ha una lunghezza minima?	NO	SI (6)	SI (6)	SI (3)	SI (8)	SI (6)	SI (6)	SI (6)	SI (8)	NO	SI (3)
Tentativi di prova della password prima che lo USERID sia disabilitato		5			3	5	5	5		3	

I profili di abilitazione disponibili per le diverse applicazioni sono riportati invece nel modello SICURDAT/B.

1.2.5 Utilizzo della rete internet

Il sistema informativo dell'Ateneo ed i dati in esso contenuti possono subire gravi danneggiamenti per effetto di un utilizzo improprio della connessione alla rete internet; inoltre, attraverso tale rete possono penetrare nel sistema virus informatici ed utenti non autorizzati. Allo scopo di evitare questi pericoli, gli Incaricati che dispongono di PC collegati in rete (caso a) e b)), curano l'applicazione delle seguenti regole:

1) utilizzano la connessione ad internet esclusivamente per lo svolgimento dei compiti istituzionali dell'Ufficio;
2) si astengono da un uso di internet illegale o non etico;
3) rispettano l'obbligo di non collegarsi a siti con materiale illegale e/o inappropriato;
4) si astengono dall'inviare, ricevere o mostrare testi o immagini che possono essere offensivi per le persone presenti;
5) rispettano i diritti di proprietà intellettuale facendo solo copie autorizzate di programmi o dati coperti da copyright;
6) non danneggiano nè alterano il Setup o la configurazione software della propria postazione di lavoro, evitando inoltre di installare prodotti software non licenziati e/o non certificati a corredo della postazione per la specifica destinazione d'uso;
7) rispettano la privacy delle altre persone non facendosi passare per un altro utente della rete, non tentando di modificare o accedere a file, password o dati che appartengono ad altri, non cercando di disattivare il controllo di autorizzazione all'accesso a qualunque sistema o rete di computer;
8) non diffondono messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi (catene di S. Antonio) e non inoltrano o diffondono messaggi che annunciano nuovi virus;
9) sono responsabili dell'uso della casella di posta elettronica istituzionale loro assegnata, non utilizzano le caselle di posta elettronica istituzionali per fini privati o personali, limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati, scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;
10) non utilizzano servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (http), posta elettronica e trasferimento files;
11) sono a conoscenza degli articoli del Codice Penale 615 ter – "*Accesso abusivo ad un sistema informatico o telematico*", 615 quater – "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*", 615 quinquies – "*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", nonché del Decreto legge 22 marzo 2004 n.72 convertito in legge con modificazioni dalla Legge 21 maggio 2004 n.128, (Legge Urbani) che sanziona la condivisione e/o la fruizione di file relativi ad un'opera cinematografica o assimilata protetta dal diritto d'autore.

1.2.6 Utilizzo di supporti rimovibili

E' sconsigliata la scrittura di dati sensibili e giudiziari su supporti rimovibili (floppies, DVD, dispositivi USB, CDROM, CD riscrivibili, etc.). Qualora se ne ravvisi l'indispensabilità, è necessario ridurre al minimo la permanenza di tali dati sul dispositivo utilizzato e, al termine del trattamento effettuato, provvedere:

- alla loro cancellazione mediante tecniche che li rendano non intelligibili e ricostruibili, se riutilizzati per differenti trattamenti,
  oppure,

- alla loro distruzione,
  oppure,
- alla loro conservazione secondo quanto prescritto al successivo punto 1.3.

1.3 Trattamenti non automatizzati

L'autorizzazione al trattamento di dati personali, sensibili e giudiziari effettuato senza l'ausilio di strumenti elettronici è richiesta dal Responsabile mediante il modello SICURDAT/A.

L'allegato A **,** in aggiunta alle disposizioni di carattere generale valide per tutti i trattamenti non automatizzati di seguito riportate, contiene le "DISPOSIZIONI RELATIVE AL PROTOCOLLO E AGLI ARCHIVI".

1.3.1 Dati comuni

I Responsabili del trattamento dei dati provvedono ad attuare le misure di protezione tese ad evitare l'accesso a persone non autorizzate ad archivi contenenti dati personali. Tra le misure utilizzabili si individuano le seguenti misure minime:

1) la sistemazione degli archivi e dei fascicoli in locali protetti da serrature;
2) l'utilizzo di mobili muniti di serrature per la raccolta e la conservazione dei fascicoli e dei documenti;
3) l'utilizzo di armadi ignifughi per la conservazione dei supporti informatici sui quali siano presenti copie di archivi contenenti dati personali.

Le misure di protezione di cui ai punti 1) e 2) sono **obbligatorie**, la misura di protezione individuata al punto 3) è da considerarsi opzionale.

Gli Incaricati del trattamento dei dati evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al Responsabile del trattamento dei dati.

1.3.2 Dati sensibili e giudiziari

E' obbligatorio conservare i dati solo in contenitori appositamente individuati, evitando dunque di collocare i documenti o i supporti informatici che li contengono in luoghi diversi, o di lasciarli fuori dagli stessi. In particolare non è consentito lasciare le pratiche contenenti dati sensibili sulla scrivania o comunque a portata di mano se non per il tempo necessario all'effettivo utilizzo, al termine del quale i documenti vanno comunque riposti.

Ogni Incaricato deve riporre i documenti o i supporti informatici contenenti dati sensibili o giudiziari negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, i documenti devono essere riposti o negli armadi o nei cassetti e chiusi a chiave.

I dati idonei a rivelare lo stato di salute o la vita sessuale devono essere conservati separatamente dagli altri dati.

I PIN degli studenti

Fra i dati personali vanno annoverati i PIN degli studenti attraverso la cui conoscenza (associata alla conoscenza del numero di matricola) è possibile accedere a tutti i dati dello studente, ivi compresi quelli relativi ad eventuali situazioni di handicap e quindi sensibili.

E', pertanto, opportuno che gli elenchi contenenti i PIN, forniti alle Segreterie studenti dallo CSI, vengano utilizzati e conservati con tutte le cautele del caso che i responsabili provvederanno ad individuare.

1.4 Videosorveglianza

Il Garante per la protezione dei dati personali, con apposito provvedimento, ha fornito le indicazioni da seguire ai fini di una corretta gestione dei sistemi di videosorveglianza. In attuazione di detto provvedimento, si riportano di seguito le disposizioni da osservare:

- il Responsabile dovrà verificare che i sistemi di video sorveglianza non costituiscano mezzo di controllo a distanza dei lavoratori, in ossequio alla disposizione di cui all'art. 4 della legge 300/1970;
- il Responsabile dovrà, inoltre, garantire che le immagini riprese siano visualizzate soltanto dagli Incaricati (dipendenti dell'Ateneo o soggetti esterni) appositamente nominati, esclusivamente per finalità di tutela dei beni e delle persone che si trovano nelle Sedi sorvegliate. Dovrà garantire, altresì, che le immagini registrate siano conservate per un periodo non superiore alle 24 ore. La visualizzazione delle immagini registrate dovrà avvenire esclusivamente nel caso in cui si verifichi un illecito o in relazione ad indagini dell'autorità giudiziaria o di polizia;
- il Responsabile dovrà, infine, rendere alle persone che possono essere riprese idonea informativa, ai sensi dell'art. 13 del Codice, circa la presenza degli impianti, curandosi di affiggere appositi cartelli nei luoghi ripresi dalle telecamere; dovrà, in particolare, indicare le finalità e le modalità del trattamento, precisando le modalità di conservazione e visualizzazione delle immagini e i nominativi dei soggetti autorizzati a tali operazioni, secondo il modello di seguito riportato:

INFORMATIVA
(ai sensi dell'art. 13 del D.Lgs 196/2003)

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali si informa che in questo locale è presente un impianto di videosorveglianza, installato per ragioni di sicurezza e di tutela dei beni che si trovano in questo Edificio.
Le immagini riprese possono essere visualizzate soltanto dagli Incaricati del servizio di custodia e vigilanza afferenti alla Amministrazione Centrale dell'Università degli Studi di Napoli Federico II, esclusivamente per le finalità innanzi indicate.

Le immagini registrate vengono conservate per un periodo non superiore alle 24 ore. Esse possono essere visualizzate dal Responsabile e dagli Incaricati del trattamento esclusivamente nel caso in cui si verifichi un illecito o in relazione ad indagini dell'autorità giudiziaria o di polizia.
Titolare del trattamento è l'Università degli Studi di Napoli Federico II.
Il Responsabile del trattamento è il sig/ dott. _____, Responsabile dell'Ufficio _____.

2 RACCOMANDAZIONI GENERALI

2.1 Distanza di cortesia

L'udienza degli utenti va organizzata in modo da evitare che altri, dipendenti o non dipendenti, possano, anche involontariamente, ascoltare i colloqui che ciascun utente intrattiene con il personale addetto a recepire le relative istanze. Deve, cioè, essere garantita la *c.d. distanza di cortesia* nelle ipotesi in cui vengano in rilievo dati personali dell'interessato.

2.2 Linee guida per il corretto utilizzo di userid e password

La sicurezza logica si realizza assicurando che tutti gli accessi ai diversi componenti del sistema informativo dell'Ateneo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa informatica, deve essere presente un meccanismo che costringa l'utente (responsabile o incaricato privacy) ad autenticarsi, ossia a dimostrare la propria identità, mediante tipicamente l'utilizzo di un codice identificativo personale (userid) ed una parola chiave (password).

Tutti gli utenti rispettano le seguenti disposizioni:

A) L'utente è responsabile della corretta tenuta della password di accensione del PC che gli è stato assegnato e delle eventuali password di accesso alla rete e alle applicazioni;
B) L'utente a cui è stata assegnata una userid per l'accesso alla rete e/o per l'utilizzo di applicazioni informatiche centralizzate, è responsabile di tutto quanto accade a seguito di transazioni ed elaborazioni abilitate dal proprio codice identificativo personale. Per le applicazioni informatiche centralizzate, tale responsabilità deve essere riferita ai privilegi associati al suo profilo di abilitazione;
C) L'utente cambia le proprie password secondo le disposizioni riportate nel presente manuale;
D) L'utente gestisce le proprie password secondo le disposizioni riportate nel presente manuale;
E) L'utente attiva tutte le misure in suo potere per evitare che terzi abbiano accesso al suo PC mentre si allontana durante una sessione di lavoro. A tal fine esce sempre dall'applicazione in uso (logoff) o eventualmente blocca il PC con uno screen saver protetto da password;
F) L'utente non comunica a nessun altro utente le proprie password.

In generale, vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **la password di accensione del PC** (password di BIOS) impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un qualsiasi motivo non ci si trova in Ufficio;
b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'Ufficio (stampanti, cartelle condivise);
c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato;

d) **la password di protezione delle risorse (cartelle) condivise** impedisce l'accesso a tali risorse da parte di utenti non autorizzati i cui PC siano collegati sulla stessa rete locale ed impedisce la propagazione di virus informatici nella rete locale;
e) **la password della casella di posta elettronica istituzionale** impedisce che i messaggi di posta elettronica indirizzati ad un utente possano essere letti da utenti non autorizzati;
f) **la password del salvaschermo** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

La gestione delle password indicate sono disciplinata dal **Disciplinare tecnico in materia di misure minime di sicurezza - D. Lgs. 196/03, Allegato B** (regole da 1 a 11): in sintesi, esse hanno una lunghezza non inferiore ad 8 caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo; queste password sono modificate dall' Incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari, la password deve essere modificata almeno ogni tre mesi. Le credenziali sono inoltre disattivate dopo sei mesi di mancato utilizzo e sono revocate nel caso di perdita delle qualità che consente all'utente l'accesso ai dati personali.

Le password di cui ai punti e) ed f) rappresentano un ulteriore livello di protezione il cui impiego è lasciato alla discrezione dell'utente della postazione di lavoro.

Nella gestione delle password è necessario attenersi alle indicazioni di seguito riportate.

Cosa NON fare:

1) NON comunicare a NESSUNO le proprie password, qualunque sia il mezzo che viene utilizzato per inoltrare la richiesta (telefono, messaggio di posta elettronica, ecc.). Ricordare che NESSUNO è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto o gli addetti alla manutenzione delle postazioni di lavoro, e che lo scopo principale per cui sono utilizzate le password è di assicurare che nessun altro possa utilizzare le risorse a cui si è abilitati;
2) NON scrivere le password su supporti che possano essere trovati facilmente e/o soprattutto in prossimità della postazione di lavoro utilizzata;
3) NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Esistono programmi che permettono di provare come password tutte quelle contenute in dizionari elettronici estremamente ampi, in termini di numero di lemmi, e in diverse lingue, scritte sia in senso normale che in senso inverso;
4) NON usare come password il nome utente o parole che possano essere facilmente riconducibili all'identità dell'utente, come, ad esempio, il codice fiscale, il nome del coniuge, il nome dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della strada in cui si abita, il nome della squadra di calcio per cui si tifa, ecc.;
5) NON usare come password parole ottenute da una combinazione di tasti vicini sulla tastiera o sequenze di caratteri (esempio: qwerty, asdfgh, 123321, aaabbb, ecc.);
6) NON usare la STESSA password per le diverse tipologie di password prima individuate;
7) NON rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password.

Cosa FARE:

1) Cambiare le password frequentemente ricordando che il limite massimo di validità di una password stabilito dalle presenti misure minime è di 6 mesi;
2) Utilizzare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione;
3) Nella digitazione delle password assicurarsi che non ci sia nessuno che osservi ciò che si digita sulla tastiera del PC;
4) Utilizzare password distinte per le diverse tipologie di password prima descritte.

2.3 Come scegliere le password

La scelta della password da parte dell'utente deve essere oculata in quanto il modo più semplice e più utilizzato per realizzare un accesso illecito ad un sistema e/o ad un applicazione, consiste nell'ottenere le credenziali identificative di un utente autorizzato, ossia la sua coppia userid e password. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.

Le password migliori sono quelle facili da ricordare ma, allo stesso tempo, difficili da individuare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione e caratteri maiuscoli e minuscoli. La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".

Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".

Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".
N.B. Non utilizzare come password gli esempi riportati nel presente manuale.

2.4 Sicurezza del software e dell'hardware

Se nell'utilizzo del PC e/o dell'applicazione informatica a cui si è abilitati, viene rilevato un problema che può compromettere la sicurezza dei dati, l'utente ne dà immediata comunicazione al Responsabile del trattamento che, a sua volta, provvede ad inoltrare la comunicazione, mediante help desk (al numero 76799), allo CSI. Quest'ultimo analizza il problema segnalato e adotta tutte le misure tecniche necessarie a risolverlo.

All'utente è vietato installare programmi non attinenti le normali attività d'Ufficio, né nuovi programmi necessari, senza il preventivo parere tecnico del Servizio Informatico dell'Ente. Gli utenti

non possono modificare le configurazioni hardware e software delle apparecchiature senza il preventivo parere tecnico del Servizio Informatico dell'Ente.

Gli utenti, con cadenza almeno mensile, verificano la presenza, sul sito ufficiale della Microsoft, di correzioni software per problemi di sicurezza, applicabili alla propria versione di sistema operativo. Se nel corso di tale verifica, effettuata attivando la funzione di Windows Update presente nei comandi principali del menù Start, si rileva la presenza di correzioni software per problemi di sicurezza (aggiornamenti critici), l'utente è tenuto a scaricare ed installare tali aggiornamenti sulla propria postazione di lavoro, seguendo le istruzioni riportate nel sito Microsoft. Tale adempimento è applicabile a tutti gli utenti le cui postazioni di lavoro sono collegate alla rete internet.

Tutti gli utenti evitano qualsiasi tipo di azione teso a superare le protezioni applicate ai sistemi e alle applicazioni. Gli interventi di installazione, configurazione e regolazione dei sistemi sono effettuabili solo dallo CSI. A conclusione dell'intervento di manutenzione, il Responsabile del trattamento è tenuto comunque a verificare che il PC sia riportato nella situazione originaria per quanto riguarda le misure minime (password di accensione del PC, presenza del programma antivirus).

E' espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del PC.

2.5 Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in essi presenti. Un virus informatico può danneggiare un PC, può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibile parti del sistema informativo, ivi compresa la rete di trasmissione dati.

I seguenti comportamenti inducono un aumento del livello di rischio di contaminazione da virus informatici:

1) installazione di software gratuito (freeware o shareware) prelevato da siti internet o allegato a riviste e/o libri;
2) scambio di file eseguibili allegati a messaggi di posta elettronica;
3) ricezione ed esecuzione di file eseguibili allegati a messaggi di posta elettronica;
4) collegamenti ad internet con esecuzione di file eseguibili, applets Java, ActiveX;
5) utilizzo della condivisione, senza password, di cartelle fra computer in rete;
6) utilizzo di floppy disk già utilizzati e la cui provenienza sia dubbia.

Al fine di evitare i problemi correlati alla diffusione di virus informatici, gli utenti devono rispettare, come misure minime, le seguenti norme:

1) accertarsi che sul proprio computer sia sempre operativo il programma antivirus in uso presso l'Ateneo. Nel caso contrario segnalare immediatamente la situazione al Centro Servizi Informativi d'Ateneo (CSI), tramite help desk;

2) accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati. Nel caso che il mittente del messaggio di posta elettronica dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;
3) sottoporre a controllo, con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna e/o incerti prima di eseguire uno qualsiasi dei files in esso contenuti;
4) non condividere con altri computer il proprio disco rigido o una cartella senza password di protezione in lettura/scrittura;
5) proteggere in scrittura i propri floppy disk contenenti programmi eseguibili e/o files di dati;
6) limitare la trasmissione fra computer in rete di files eseguibili e di sistema;
7) non intraprendere azioni di modifica sui sistemi utilizzati a seguito di diffusione di messaggi e segnalazioni di virus informatici da qualsiasi fonte provengano. Le uniche azioni eventualmente necessarie sono comunicate esclusivamente dal Centro Servizi Informativi d'Ateneo (CSI);
8) non scaricare dalla rete internet programmi o files non inerenti l'attività dell'Ufficio o comunque sospetti;
9) distribuire preferibilmente documenti in formato elettronico avviene tramite formati standard, compatibili e possibilmente compressi (p.e. PDF).

Allegato A - DISPOSIZIONI RELATIVE AL PROTOCOLLO E AGLI ARCHIVI

Con il precedente Ordine di Servizio n. 93 sono state dettate disposizioni relative al Protocollo e agli archivi dell'Amministrazione Centrale, che vengono, con il presente provvedimento aggiornate e di seguito riportate.

Il Protocollo

Il protocollo rappresenta, ai fini della tutela della riservatezza, un settore particolarmente delicato considerato che vi transitano tutti i documenti dell'amministrazione sia in entrata che in uscita.

Ciò implica che gli addetti all'Ufficio Protocollo ed Archivio, anche se per il solo transito di documenti, gestiscono quasi la totalità delle informazioni che vengono trattate dall'amministrazione.

Risulta dunque indispensabile che essi siano particolarmente attenti, nello svolgimento delle attività di competenza, alla problematica in oggetto.

Si ribadiscono pertanto tutte le disposizioni dettate in precedenza per il trattamento dei dati personali (sia automatizzati che non automatizzati), sottolineando alcuni aspetti ulteriori che per il settore in argomento assumono particolare rilievo:

- l'accesso all'ufficio va costantemente controllato;
- gli addetti di altre strutture devono effettuare le operazioni di prelievo e consegna di documenti nel locale d'ingresso;
- non è consentito intrattenersi presso i locali dell'ufficio se non per il tempo strettamente necessario alla consegna o al prelievo;
- l'ufficio disporrà affinché una unità di personale sia addetta al ricevimento dei documenti, evitando l'accesso all'ufficio da parte di personale di altre strutture, quando ciò non sia necessario;
- ciascun addetto al protocollo deve avere accesso ai soli documenti indispensabili allo svolgimento dei compiti assegnati.

L'archivio corrente del palazzo degli Uffici

I locali appositamente destinati all'archivio in argomento devono essere presidiati da una unità di personale afferente all'ufficio Protocollo e Archivio con mansioni di custodia e controllo sul prelievo e ricollocazione della documentazione di volta in volta occorrente agli uffici medesimi.

Il personale addetto al controllo dovrà consentire l'accesso all'archivio esclusivamente al personale munito di autorizzazione firmata dal capo dell'ufficio o del reparto ed opportunamente esibita.

I responsabili di struttura organizzano, pertanto, il servizio di prelievo, smistamento e ricollocazione della documentazione individuando, con le modalità sopra indicate, un proprio addetto che, durante l'orario di apertura al pubblico o al ricorrere delle eventuali esigenze lavorative della struttura, dovrà recarsi presso i locali adibiti ad archivio.

Gli archivi di deposito (Sede Centrale, Botteghelle, Monte Sant'Angelo)

a) L'archiviazione. La restituzione di documenti in consultazione.

I documenti da archiviare devono essere consegnati all'Incaricato dell'Ufficio Protocollo e Archivio, previo informale preavviso, ogni giovedì dalle ore 9.00 alle ore 13.00 ed in caso di festività il successivo giorno lavorativo.

Dovranno essere accompagnati dalla relativa nota di trasmissione, utilizzando il modello **ARC/1,** consultabile sul portale dell'Università, nella sezione Ateneo, alla voce amministrazione-sicurezza privacy, al seguente link www.unina.it/ateneoFridericiano/amministrazione/sicurezzaPrivacy/index.jsp, con l'indicazione dettagliata della documentazione da archiviare.

Analogo iter dovrà essere seguito per la restituzione di documentazione o fascicoli già archiviati e temporaneamente in consultazione.

Qualora la richiesta di archiviazione concerna un numero considerevole di fascicoli pacchi e contenitori, la trasmissione dovrà essere preventivamente concordata con il capo dell'Ufficio Protocollo ed Archivio e con il responsabile dei Servizi Generali. Il detto responsabile disporrà, d'intesa con il capo dell'Ufficio Protocollo ed Archivio il trasporto della documentazione in argomento dall'Ufficio interessato ai locali di archivio cui la stessa è destinata.

Alla consegna della documentazione all'Ufficio Protocollo ed Archivio dovrà presenziare un Incaricato dell'ufficio richiedente.

b) La consultazione di documenti archiviati.

La consultazione di documenti archiviati comporta normalmente l'accesso a dati personali. Pertanto si ritiene utile riportare in questa sede le disposizioni relative all'archiviazione di documenti e fascicoli.

b.1) La consultazione presso l'archivio della Sede Centrale:

Le richieste di consultazione di documenti e fascicoli archiviati nell'archivio della Sede Centrale devono essere inoltrate all'Ufficio Protocollo e Archivio, a mezzo degli appositi modelli (mod. **ARC/2**, per la consultazione di documentazione non relativa agli studenti; mod. **ARC/3**, per la consultazione di fascicoli degli studenti, disponibili sul portale dell'Università, nella sezione Ateneo, alla voce amministrazione-sicurezza privacy, al seguente link www.unina.it/ateneoFridericiano/amministrazione/sicurezzaPrivacy/index.jsp).

L'ufficio provvederà ad evadere, ove possibile, in tempo reale e in stretto ordine cronologico tutte le richieste avanzate dagli utenti ogni giovedì dalle ore 9.00 alle ore 13.00 ed, in caso di festività il successivo giorno lavorativo.

Gli stessi uffici, nel giorno e nelle ore sopra indicate, avanzeranno le opportune richieste, ritirando contemporaneamente, laddove possibile, la relativa documentazione.

Nel mese di agosto l'Ufficio Protocollo ed Archivio assicurerà il servizio nello stesso giorno e con le stesse modalità, previa richiesta telefonica da parte degli uffici interessati.

L'urgenza della richiesta, debitamente motivata, sarà valutata dal Dirigente della III Ripartizione.

Le chiavi di accesso ai locali dell'archivio devono essere consegnate dai custodi della sede centrale unicamente al personale dell'ufficio archivio che sarà opportunamente indicato dal Capo Ufficio.

b.2) La consultazione presso gli archivi di via Botteghelle e di Monte Sant'Angelo

Le richieste relative a documentazione e fascicoli conservati negli archivi di via Botteghelle e di Monte Sant'Angelo devono essere inoltrate attraverso i modelli **ARC/2** e **ARC/3**, come sopra specificato.

L'evasione delle richieste avverrà in stretto ordine cronologico, fatte salve le motivazioni di urgenza opportunamente indicate e valutate dal Dirigente della V Ripartizione.

L'ufficio Protocollo ed Archivio provvederà a trasmettere i fascicoli e la documentazione richiesti con un apposito elenco riportante la indicazione dell'ufficio richiedente.

Il responsabile dei Servizi Generali disporrà affinché siano prelevati ogni mercoledì i fascicoli e la documentazione per la relativa consegna; provvederà, altresì, a restituire all'Ufficio Protocollo ed Archivio copia dell'elenco di trasmissione di cui sopra, completo delle firme di ricevuta.

Eventuali autorizzazioni di accesso ai locali adibiti ad archivio in deroga alle presenti disposizioni saranno concesse, di volta in volta, per iscritto, dal capo dell'Ufficio Protocollo e Archivio, che provvederà a conservare copia della richiesta e della autorizzazione.

I fascicoli consultati devono essere utilizzati secondo le modalità dettate per i documenti contenuti negli archivi correnti.