MANUALE AD USO DEI RESPONSABILI E DEGLI INCARICATI

1) Sicurezza fisica

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 la sistemazione degli archivi e dei fascicoli in locali protetti da serrature, l'utilizzo di mobili muniti di serrature per la raccolta e la conservazione dei fascicoli e dei documenti, l'utilizzo di armadi ignifughi per la conservazione dei dati, ecc.

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

2) Sicurezza logica

La sicurezza logica si realizza principalmente assicurando che tutti gli accessi ai diversi componenti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa, deve essere previsto un meccanismo che costringa l'utente 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 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 si riferisce ai privilegi associati al suo profilo di abilitazione;
C) L'utente cambia le proprie password secondo le disposizioni riportate nelle misure minime e nel presente manuale;
D) L'utente gestisce le proprie password secondo le disposizioni riportate nelle misure minime e 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) ed eventualmente blocca il PC con la password di uno screen saver;
F) L'utente non comunica a nessun altro utente le proprie password.

Nell'ambito delle presenti misure minime, sono individuati i seguenti livelli di protezione:

- password di accensione del PC (password di BIOS);
- userid e password per l'accesso alle risorse di rete;
- userid, password e profili di abilitazione per le applicazioni informatiche centralizzate.

2.1) Istruzioni sull'utilizzo delle password e dei codici identificativi personali

Password di accensione del PC (password di BIOS)
Tutti gli utenti che utilizzano un PC, anche non collegato in rete, devono identificarsi con password, al momento dell'accensione del PC, utilizzando una funzionalità del BIOS del PC. Le regole applicabili alla password di BIOS sono riportate nella Tabella 1.

DESCRIZIONE	REGOLA
La password di BIOS può essere modificata dall'utente?	SI
Quale è la durata della password di BIOS?	6 mesi
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 1 – Regole valide per l'utilizzo della password di BIOS

Codice identificativo personale (userid) e password per l'accesso alle risorse di rete

Oltre all'identificazione appena descritta, tutti gli utenti che utilizzano PC collegati sulla rete dell'Amministrazione, per poter accedere alle risorse presenti nella propria rete (stampanti e cartelle), devono identificarsi, con userid e password, al momento del collegamento. Questa verifica dell'identità dell'utente si aggiunge all'identificazione descritta in precedenza, nel senso che è operativa a prescindere dal fatto che l'utente sia o meno utilizzatore di una o più delle applicazioni informatiche prima elencate. Le regole applicabili allo userid e alla password di rete, sono riportate nella Tabella 2.

DESCRIZIONE	REGOLA
La password di rete può essere modificata dall'utente?	SI
Quale è la durata della password di rete?	90 gg.
Lo userid viene revocato in caso di mancato utilizzo?	NO
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

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

Codice identificativo personale (userid) e 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/2 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 CEDA 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).

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.

	ASIB	**ASIP**	**GEDAS**	**SIOC**	**SIPR**	**FINUNI**	**FISC**	**GTIK**	**PRES**	**VALCOM**
Livelli di identificazione	1	1	1	1	1	2	2	2	2	1
La password può essere modificata dall'utente?	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO
Quale è la durata della password ?		30 gg.	30 gg.			30 gg.	30 gg.	30 gg.	30 gg.	60gg.

	ASIB	ASIP	GEDAS	SIOC	SIPR	FINUNI	FISC	GTIK	PRES	VALCOM
Livelli di identificazione	1	1	1	1	1	2	2	2	2	1
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.	SI, dopo 45 gg.	
La password ha una lunghezza minima?	NO	SI (6)	SI (6)	SI (3)	SI (3)	SI (6)	SI (6)	SI (6)	SI (6)	NO
Quanti sono i tentativi di prova della password prima che lo USERID sia disabilitato?		5				5	5	5	5	3

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

I profili di abilitazione disponibili per le diverse applicazioni sono riportati invece nel modello SICURDAT/2.

Linee guida per il corretto utilizzo delle password

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. La password di accensione ha una lunghezza non inferiore a **6 caratteri** e deve essere aggiornata almeno ogni **6 mesi**;

b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'Ufficio (stampanti, cartelle condivise). La password di rete ha una lunghezza non inferiore a **8 caratteri** e deve essere aggiornata almeno ogni **3 mesi**;

c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato. Per la lunghezza delle password delle applicazioni informatiche centralizzate e per la frequenza di aggiornamento, fare riferimento alla Tabella 1;

d) **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;

e) **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.

Le password indicate ai punti a), b) e c) sono disciplinate dalle misure minime. Le password di cui ai punti d) ed e) rappresentano invece un ulteriore livello di protezione il cui impiego è lasciato alla discrezione dell'utente della postazione di lavoro.

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. Considerato che per molte applicazioni informatiche centralizzate, lo userid coincide con la matricola del dipendente ed è quindi un dato noto, l'intera sicurezza si basa sulla conoscenza della password. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.

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, 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 (password di accensione del PC);
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.

Come scegliere le password

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.

3) 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 al CEDA. 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 CEDA. Gli utenti non possono modificare le configurazioni hardware e software delle apparecchiature senza il preventivo parere tecnico del CEDA.

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 dal personale tecnico del CEDA o, nel caso di riparazioni hardware, dalla ditta cui è affidato il servizio di manutenzione delle apparecchiature periferiche. Nel caso di intervento tecnico effettuato dalla ditta a cui è affidato il servizio di manutenzione, il Responsabile del trattamento è tenuto a verificare che al termine dell'intervento il PC sia riportato nella situazione originaria per quanto riguarda le misure minime (password di accensione, presenza del programma antivirus). E' espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del PC.

4) 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:

A) installazione di software gratuito (freeware o shareware) prelevato da siti internet o allegato a riviste e/o libri;
B) scambio di file eseguibili allegati a messaggi di posta elettronica;
C) ricezione ed esecuzione di file eseguibili allegati a messaggi di posta elettronica;
D) collegamenti ad internet con esecuzione di file eseguibili, applets Java, ActiveX;
E) utilizzo della condivisione, senza password, di cartelle fra computer in rete;
F) 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'Amministrazione;
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 di files 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 CEDA;
8) non scaricare dalla rete internet programmi o files non inerenti l'attività dell'Ufficio o comunque sospetti.

Dal punto di vista operativo, occorre considerare che:

1) tutti i PC dell'Amministrazione sono dotati di programma antivirus. Il programma antivirus, per i PC collegati in rete, viene aggiornato automaticamente con cadenza giornaliera. Per i PC non collegati in rete l'aggiornamento del programma antivirus viene effettuato con cadenza almeno mensile da parte del personale tecnico del CEDA;
2) al momento dell'individuazione di un virus informatico sul PC da parte del programma antivirus, l'utente 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 al CEDA l'evento per eventuali e successivi interventi tecnici;
3) la distribuzione di documenti in formato elettronico avviene tramite formati standard, compatibili e possibilmente compressi (p.e. PDF).

5) Utilizzo della rete internet

Il sistema informativo dell'Amministrazione 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 utenti curano l'applicazione delle seguenti regole:
1) gli utenti utilizzano la connessione ad internet esclusivamente per lo svolgimento dei compiti istituzionali dell'Ufficio;
2) gli utenti 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;
3) le caselle di posta elettronica rilasciate dall'Amministrazione non vengono utilizzate dagli utenti per fini privati o personali. Gli utenti sono responsabili dell'uso della casella di posta elettronica istituzionale loro assegnata;
4) gli utenti limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati, scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;
5) è vietato l'utilizzo di servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (http), posta elettronica e trasferimento files;
6) gli utenti devono essere 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 telematic*i", 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.