Regolamento per l'utilizzo degli strumenti informatici

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento indica le modalità di utilizzo degli strumenti informatici aziendali in dotazione agli operatori, con particolare riferimento agli aspetti connessi alla tutela dei dati in essi presenti ed alla salvaguardia dei dispositivi informatici.

Il presente documento sarà oggetto di monitoraggio e aggiornamento periodico da parte dell'USC Informatica e telecomunicazioni al fine di garantirne l'efficacia applicativa e l'attualità.

2. TERMINOLOGIA E ABBREVIAZIONI

ACCESS POINT	È un dispositivo elettronico di telecomunicazioni che permette all'operatore mobile di collegarsi ad una rete wireless direttamente tramite il suo terminale se dotato di scheda wireless.
ASST	Azienda Socio Sanitaria Territoriale
BROWSER	È un programma che consente di visualizzare i contenuti delle pagine dei siti web e di interagire con essi, permettendo così all'operatore di navigare in Internet. Il browser da utilizzare presso l'ASST "Papa Giovanni XXIII" è Internet Explorer, essendo l'unico browser certificato per l'utilizzo delle applicazioni aziendali.
CREDENZIALI DI AUTENTICAZIONE	Per l'accesso ai Personal Computer e agli applicativi le credenziali coincidono con il PIN della smartcard personale (aziendale o SISS-operatore)
DOWNLOAD	È l'azione di ricevere o prelevare dalla rete (es. da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'operatore
SINGLE SIGN ON (SSO)	È un sistema specializzato che permette ad un operatore di autenticarsi una sola volta e di accedere a tutte le risorse informatiche alle quali è abilitato. Tale accesso avviene mediante la smartcard personale (aziendale o SISS-operatore).
INTRANET	È una rete locale (LAN), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso all'informazione, che può essere ad accesso ristretto. All'interno dell'Intranet vengono acceduti i programmi aziendali (applicazioni dipartimentali).
LAN	Local Area Network. È una tipologia di rete informatica contraddistinta da un'estensione territoriale non superiore a qualche chilometro.
LOG	La registrazione cronologica delle operazioni che vengono eseguite su un sistema informatico. Rappresenta l'evidenza informatica che dimostra che una certa elaborazione è avvenuta.
MALWARE	Un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito
PASSWORD	È una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa che ne richieda l'uso o per effettuare operazioni di firma elettronica.
PDL	Postazione di lavoro (personal computer o notebook o laptop)

PIN	Il PIN (Personal Identification Number) è un codice alfanumerico che serve a proteggere la smartcard (e quindi l'accesso a Personal Computer e applicativi) da utilizzi illeciti. Se viene digitato erroneamente per 3 volte di seguito, è necessario inserire il codice PUK (PIN UNBLOCKED KEY). Sostituisce l'utilizzo della coppia USER ID e PASSWORD, e rappresenta la modalità standard di accesso alle risorse informatiche. Il PIN non deve mai essere comunicato a terzi, e rappresenta, nel paradigma di autenticazione informatica a due fattori, il secondo fattore autenticativo.
SPAM	Lo spamming (detto anche fare spam) è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque mezzo informatico, ma il più usato è Internet, attraverso l'e-mail.
SSO	Single Sign On, sistema di gestione delle credenziali di accesso
TROJAN HORSE	È un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'operatore stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto
UPLOAD	È il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica.
USER ID	Codice che identifica univocamente un operatore all'interno di un sistema informatico; Lo USER ID (matricola aziendale) viene creato dall'USC ICT e non può essere modificato.
VIRUS	Un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'operatore. Generalmente causa danno ai sistemi informatici
VLAN (VIRTUAL LAN)	Un insieme di tecnologie che permettono la suddivisione di un insieme di computer collegati ad un'unica rete in più reti virtuali (più facilmente gestibili)
WHITE LIST	Modalità di governo del controllo accessi alle risorse informatiche che consiste nel permettere l'accesso alle risorse espressamente elencate nella lista, vietando l'accesso alle risorse non presenti in elenco.
WIRED	Comunicazione tra dispositivi elettronici collegati fra di loro attraverso un apposito cavo;
WIRELESS	Il termine wireless (dall'inglese senza fili) indica una comunicazione tra dispositivi elettronici che non fa uso di cavi.
WLAN	Indica una "rete locale senza fili" che sfrutta la tecnologia wireless. Si indicano genericamente tutte le reti locali di computer che non utilizzano dei collegamenti via cavo (wired) per connettere fra loro i computer alla rete.

3. DESTINATARI

Il documento è rivolto a tutti coloro che utilizzano strumenti informatici nello svolgimento di attività sanitarie, amministrative e tecniche e, in particolare, a tutti coloro che trattano dati personali a titolo di Responsabile e Incaricato del trattamento, ai sensi del D.lgs. n. 196/2003.

Esso si prefigge lo scopo di rendere consapevoli gli utilizzatori interni ed esterni dell'azienda (i Responsabili e gli Incaricati del trattamento), in merito al trattamento dei dati con strumenti elettronici e alle modalità di utilizzo degli strumenti informatici aziendali (ad esempio Personal Computer, rete interna, posta elettronica, Internet).

4. TRATTAMENTO DATI

4.1 Credenziali di autenticazione

Le credenziali di autenticazione si suddividono in credenziali di autenticazione per l'accesso al dominio aziendale (vedi paragrafo 4.1.1) e credenziali di autenticazione per l'accesso agli applicativi aziendali (vedi paragrafo 4.1.2).

4.1.1 Credenziali di autenticazione al dominio aziendale

L'ASST ha acquisito un sistema di gestione delle credenziali per l'accesso ai Personal Computer e agli applicativi aziendali noto con il nome di Enterprise Single Sign On (ESSO o SSO).

Tale meccanismo di sicurezza, basato sull'utilizzo di una carta a microprocessore, delega la gestione delle credenziali ad un sistema informatico, garantendo la sicurezza degli accessi personali agli operatori da una parte, e garantendo altresì che i dati di accesso degli interessati siano trattati solo dagli aventi diritto.

Per dominio aziendale si intende l'insieme di risorse informatiche (Personal Computer, stampanti, ecc.) messe a disposizione dall'ASST per la comunicazione all'interno della rete locale (LAN).

L'accesso al Personale Computer avviene tramite utilizzo di smartcard.

Ogni operatore dovrà possedere le proprie credenziali di autenticazione al dominio e dovrà sempre accedere tramite le predette credenziali.

Con "credenziali di autenticazione al dominio" si intende il PIN della smartcard che viene richiesto in fase di accesso al Personal Computer (in seguito all'accensione o successivamente alla disconnessione di un operatore precedentemente connesso).

Nel caso in cui sia necessario richiedere un ripristino del PIN, è necessario seguire le istruzioni contenute nel manuale apposito (vedi allegato n. 1 "Slocco_Cambio_PIN.pdf" al presente documento) oppure aprire una chiamata al sistema di Help Desk aziendale.

4.1.2 Eccezioni in fase di autenticazione al dominio aziendale

Sono possibili due modalità alternative di accesso al dominio aziendale, qui riportate:

1. accesso mediante postazioni cosiddette di 'autologin': è una modalità di accesso automatico - ossia senza la necessità di autenticazione con smartcard - che è stata fornita in via eccezionale per rispondere a specifiche necessità operative. Tale modalità non permette l'accesso alle cartelle condivise e laddove possibile è oggetto di restrizioni a livello di funzionalità (es. accesso ad Internet, possibilità di accesso a particolari risorse di rete, ecc.). Dal momento che questa modalità per definizione non è associata ad un'autenticazione personale, non è mai da ritenersi preferibile all'accesso via smartcard e non è possibile impostare nuove postazioni di lavoro affinchè accedano al dominio in tale modalità. Se da una postazione in modalità 'autologin' si volesse accedere alle proprie cartelle in rete è necessario disconnettere l'utente di tipo 'autologin' ed autenticarsi con la propria smartcard. Per accedere alle applicazioni aziendali è sempre necessario inserire nel lettore la propria smartcard personale (Single Sign On);
2. accesso mediante modalità 'cardless': rappresenta anch'essa un'eccezione alla modalità standard (ossia accesso mediante smartcard) per accedere alle postazioni di lavoro. Più precisamente si tratta di una funzionalità messa a disposizione dal sistema di autenticazione con smartcard, dove però l'accesso alla postazione di lavoro avviene mediante inserimento manuale di username (matricola aziendale) e password sicura. In tal modo è obbligatoria la disconnessione manuale dalla postazione di lavoro una volta che ci si sposta altrove, in quanto l'accesso alle applicazioni aziendali non è più protetto dall'estrazione della smartcard personale dal lettore di smartcard.

Le eccezioni suddette vengono applicate solo in seguito a specifica richiesta del Responsabile di ciascuna Struttura/Servizio., via mail al servizio di HelpDesk (helpdesksio@asst-pg23.it) oppure tramite il software aziendale "Easy Vista" come da nostre istruzioni che di volta in volta verranno condivise e valutate congiuntamente con l'USC ICT.

Esempio:

Qualora si presenti l'esigenza, presso specifiche aree, di dover accedere alle informazioni cliniche escludendo l'utilizzo di accesso a cartelle condivise (bypassando l'autenticazione personale sul personal computer) e l'accesso ai dispositivi ubicati presso quelle aree sono ad accesso selezionato – viene quindi garantita la sicurezza fisica ai locali -, l'eccezione può essere considerata legittima.

4.1.3 Credenziali di autenticazione per l'accesso agli applicativi aziendali

Il trattamento dei dati personali con strumenti elettronici è consentito ai Responsabili ed Incaricati dotati di credenziali di autenticazione personali per l'accesso agli applicativi aziendali (ad esempio BOOK, GALILEO, OLIAMM, FARMASAFE@, ecc.).

Le credenziali di autenticazione consistono in una smartcard e nel relativo PIN.

Le credenziali di autenticazione possono essere una o più ma sempre assegnate o associate individualmente e sempre accedibili esclusivamente attraverso la propria smartcard.

Di fatto non vi è più, da parte degli utilizzatori dei sistemi informatici, l'onere di custodire le password in modo che siano rispondenti ai criteri di robustezza in termini di lunghezza e complessità (come richiesto dalla normativa vigente).

L'unica credenziale che andrà custodita dall'operatore è quindi il PIN associato alla carta, modificato dall'operatore stesso al primo accesso oppure anche successivamente. Nella scelta del PIN non devono essere utilizzati riferimenti personali (ad esempio nome, cognome, data di nascita, ecc.).

L'utilizzo della smartcard prevede che il riconoscimento dell'operatore avvenga all'accensione del Personal Computer e successivamente solo all'apertura del primo applicativo; eventuali altre applicazioni aziendali verranno aperte automaticamente (mediante doppio clic sull'icona).

Qualora la smartcard venga rimossa e reinserita, occorrerà ridigitare il proprio PIN segreto, a garanzia del fatto che chi sta utilizzando la smartcard ne sia il legittimo possessore.

Tale modalità di accesso si intende valida al netto di quelle applicazioni aziendali dove, per scelta condivisa con l'ICT e la Direzione, si è optato per un accesso con username e password sicura.

Tipicamente tale modalità è stata conservata per le applicazioni che vengono utilizzate su postazioni di lavoro protette in altro modo (es. sicurezza fisica).

5. CORRETTA CONSERVAZIONE DELLE PASSWORD E DEI DISPOSITIVI DI ACCESSO

L'operatore è tenuto a conservare nella massima segretezza il PIN per l'accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione (ossia la propria smartcard).

Quanto sopra è espressamente contenuto nell'informativa mostrata in fase di presa servizio e liberamente scaricabile, dove si informa che è obbligatorio conservare diligentemente la propria smartcard e relativo PIN, che non deve mai essere ceduta o comunicata a terzi.

Essendo la gestione delle credenziali demandata al sistema SSO, la gestione sicura deve essere garantita solamente per il PIN associato alla smartcard.

Inoltre l'operatore è tenuto a scollegarsi dal Personal Computer ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per esempio perché impegnato in compiti che richiedono totalmente la sua attenzione).

In questi casi è necessario salvare eventuali file aperti per evitare di perdere il lavoro effettuato, dal momento che l'estrazione della smartcard dal lettore comporta la disconnessione dell'operatore dal Personal Computer.

Occorre prestare anche particolare attenzione alle stampe prodotte con sistemi informatizzati: i documenti stampati devono essere presidiati o collocati in locali ad accesso controllato.

L'operatore è tenuto quindi a rimuovere la smartcard dall'apposito lettore ogni qualvolta sia costretto a lasciare incustodita la postazione di lavoro.

6. DELEGA APPLICATIVA

È possibile accedere ad una o più applicazioni aziendali a nome di un diverso Responsabile o Incaricato, per un periodo di tempo obbligatoriamente predefinito, così come previsto dalla corrente normativa in materia di protezione dei dati personali e sensibili.

Tale funzionalità, conosciuta con il nome di delega applicativa, viene resa disponibile dal sistema SSO.

La delega applicativa va considerata un evento eccezionale e viene concessa solo ed esclusivamente quando non vi siano altre opzioni percorribili.

Nello specifico, un operatore (delegato) collegato al Personal Computer con la propria smartcard può, temporaneamente, accedere agli applicativi aziendali in nome e per conto di un secondo operatore (delegante).

Esempio:

- la segretaria di un reparto può accedere alla posta elettronica del proprio primario anche se connessa al Personal Computer con la propria smartcard ;
- l'operatore X, che svolge un lavoro con il proprio account non derogabile e indispensabile, si assenta per vari motivi e per un periodo variabile di tempo. Durante tale periodo è comunque necessario che l'attività venga eseguita. In questo caso ove esiste un impedimento viene delegata un'altra persona per l'effettuazione della suddetta attività.

Condizione necessaria affinché venga concessa una delega applicativa è l'invio, da parte del Direttore/Responsabile di Struttura, di una email di richiesta, alla Segreteria dell'Ufficio Gestione Identità Digitali – UGID – (segreteriaugid@asst-pg23.it) con le seguenti informazioni:

- nome, cognome e matricola del soggetto delegante;
- nome, cognome e matricola di tutti i soggetti delegati;
- applicativi per i quali si chiede la delega;
- motivazione per la quali si richiede la delega;
- durata della delega (indicare con precisione le date di inizio e fine delega).

Ad email ricevuta, se non sussistono impedimenti di altra natura, verrà applicata la delega per lo stretto tempo necessario.

7. UTILIZZO STRUMENTI INFORMATICI

7.1 Utilizzo del Personal Computer

Il computer che l'operatore ha ricevuto in dotazione è uno strumento di lavoro, fornito dall'ASST, il cui utilizzo deve avvenire nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo aziendale e/o previste dalla legge.

Ogni utilizzo non conforme può causare disservizi, costi di manutenzione, minacce alla sicurezza, danni a persone o al patrimonio aziendale.

Le caratteristiche hardware e software del computer sono impostate dall'USC Informatica e telecomunicazioni in base alle direttive aziendali e non devono mai essere modificate autonomamente, anche nei casi in cui si posseggano i privilegi necessari.

Attualmente ogni Personal Computer aziendale in rete al quale si acceda con la propria smartcard ha automaticamente accesso ad Internet, a meno di esplicite disposizioni contrarie al riguardo.

È presente un meccanismo di sicurezza che prevede la configurazione, non modificabile dall'utilizzatore, del filtro per le connessioni ad Internet effettuate dai Personal Computer attraverso la rete aziendale.

L'utente, salvo eccezioni autorizzate dalla USC IT, non ha diritti di amministratore sul Personal Computer e per ogni attività che richieda il privilegio di amministrazione (ad esempio installazione di software, stampanti, etc) , deve riferirsi all' HelpDesk aziendale.

Eventuali restrizioni di accesso ad Internet (per esempio applicando eventuali whitelist) sono a discrezione dell'USC Informatica e telecomunicazioni se motivate da oggettivi rischi che necessitano di essere mitigati.

È vietata l'installazione di programmi diversi da quelli autorizzati dall'USC Informatica e telecomunicazioni, che può altresì procedere alla rimozione di file o applicazioni pericolose per la sicurezza.

È inoltre vietato riprodurre o duplicare materiale informatico, di qualsiasi genere, in ottemperanza alla corrente legislazione vigente in materia.

7.1.1 Pausa / fine sessione lavorativa

Durante la sessione di utilizzo del Personal Computer e al termine della stessa gli operatori non devono lasciare incustodito e accessibile con le proprie credenziali (smartcard) il dispositivo.

In particolare:

- il Personal Computer deve essere spento al termine della sessione lavorativa (fine giornata lavorativa);
- deve essere estratta la smartcard dal lettore del Personal Computer sul quale si sta effettuando l'attività lavorativa in pausa pranzo e ogniqualvolta l'operatore abbandoni la propria postazione di lavoro per un consistente periodo di tempo.

7.1.2 Dispositivi Mobili

L'operatore è responsabile del dispositivo mobile assegnatogli dall'ASST. Esso deve essere custodito con diligenza durante gli eventuali spostamenti ed al termine della giornata lavorativa deve essere riposto in un luogo sicuro, opportunamente spento.

Qualora fosse necessario, per motivi lavorativi, accedere ad Internet (web mail aziendale, siti istituzionali), l'operatore dovrà presentare richiesta all'USC Informatica e telecomunicazioni tramite il software aziendale EasyVista.

I dispositivi mobili aziendali, trasportati per ragioni di servizio all'esterno, sono dotati di opportuno software antivirus (ed altro software di sicurezza). La corretta configurazione dei Personal Computer è a cura dell'USC Informatica e telecomunicazioni.

8. USO DELLA RETE

8.1 Internet

L'ASST definisce i criteri e le modalità operative di accesso e utilizzo del servizio Internet da parte degli operatori autorizzati.

L'ASST si riserva di adeguare in qualsiasi momento le proprie politiche di sicurezza in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità.

L'operatore non può accedere a Internet per perseguire scopi privati e/o vietati dalla legge ma solo per ragioni di lavoro al fine di raggiungere obiettivi di studio, ricerca e documentazione in relazione alle specifiche mansioni e alle specifiche competenze attribuite all'interno dell'ASST.

L'ASST può adottare modalità finalizzate a bloccare l'accesso a siti ritenuti non consoni allo svolgimento dell'attività lavorativa e/o comunque non affidabili. Può altresì definire la modalità di accesso ad Internet attraverso l'utilizzo di " whitelist".

Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet tramite la rete aziendale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, ecc.).

È vietato scaricare programmi da siti Internet; in caso di necessità è opportuno rivolgersi all'USC Informatica e telecomunicazioni per avere l'autorizzazione e la necessaria assistenza tecnica.

Non è consentito fornire a soggetti non autorizzati l'accesso alla connessione Internet aziendale.

La banda impiegata per la connessione Internet è una risorsa limitata. Ogni operatore ha la responsabilità di non compiere operazioni che monopolizzino le risorse informatiche dell'ASST (eccessivo traffico in download/upload).

L'utilizzo del servizio di accesso ad Internet termina d'ufficio allorché venga meno la condizione di operatore autorizzato, non venga confermata l'autorizzazione d'uso, oppure questa venga revocata a seguito di accertamento diretto di attività non consentita o su segnalazione dell'autorità giudiziaria.

Il materiale raccolto e quello eventualmente esistente per effetto di conservazione sarà uno strumento per l'attività di controllo, come descritto nell'apposito capitolo.

I log relativi alle pagine web visitate dall'interno dell'ASST verranno conservati per un tempo massimo pari a 90 giorni, decorsi i quali verranno cancellati.

9. USO DELLA POSTA ELETTRONICA

9.1 Finalità

La casella di posta, assegnata dall'ASST all'operatore, è uno strumento di lavoro e come tale deve essere utilizzata per perseguire fini istituzionali.

Gli operatori assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Non è consentito fornire a soggetti terzi non autorizzati l'accesso al servizio di posta elettronica aziendale.

L'assegnazione di un indirizzo di posta elettronica comporta l'obbligo di utilizzo ai soli fini di supporto dell'attività lavorativa.

Ogni operatore è tenuto ad accedere alla casella e-mail assegnatagli utilizzando le proprie credenziali di autenticazione.

L'utilizzo della posta elettronica cessa d'ufficio allorché venga meno la condizione di operatore autorizzato.

9.2 Corretto Utilizzo

Chiunque utilizzi la posta elettronica è tenuto ad adottare tutte le misure idonee per non interferire nel corretto funzionamento della stessa e per assicurare agli altri utenti il godimento del medesimo servizio.

Al fine di evitare inutile traffico di rete e dispendio di risorse sul sistema posta, gli allegati ai messaggi di posta elettronica non devono, laddove possibile, consistere in file di grandi dimensioni.

È buona regola la periodica 'pulizia' della casella di posta, con la cancellazione di e-mail obsolete ed inutili.

I file ottenuti da fonti esterne alla rete aziendale, inclusi gli allegati ai messaggi di posta elettronica, sono spesso veicolo di software malevolo.

Il server di posta elettronica interno all'ASST è dotato di strumenti di protezione logica costantemente aggiornati ed atti a contenere i rischi derivanti da possibili incidenti informatici. Resta evidentemente in capo ad ogni singolo operatore la responsabilità di un atteggiamento consapevole nei confronti di tali insidie.

Gli utilizzatori del servizio di posta elettronica non devono pertanto aprire, per nessuna ragione, email aventi mittente, oggetto o allegati incerti o sospetti. In questi casi è obbligatorio cancellare il messaggio di posta.

L'Azienda utilizza opportuni sistemi antispam ed antivirus, ossia dei sistemi che consentono di bloccare la propagazione di spam e virus, ed eventuali azioni illecite, per quanto possibile. I messaggi "taggati" come [SPAM] sono messaggi identificati dal sistema come messaggi indesiderati, per cui si invita a verificarne la provenienza e valutare la loro cancellazione.

È espressamente vietato qualsiasi utilizzo della posta elettronica che possa tradursi in un danno o semplicemente in un disturbo a terzi; ad esempio l'invio indiscriminato di messaggi di posta elettronica indirizzati ad un medesimo soggetto, la diffusione via e-mail di materiale pubblicitario e/o commerciale non richiesto (spamming), "catene di S. Antonio", ecc..

Non è consentito, all'amministratore del sistema di posta, leggere e registrare sistematicamente i messaggi di posta elettronica, al di là di quanto tecnicamente necessario per svolgere il proprio servizio di amministrazione del sistema.

Gli allegati di grande dimensione (dimensione uguale o superiore ad 1 MB) devono essere trasmessi in formato compresso (zip, rar). Attualmente non è possibile ricevere o spedire messaggi di posta con allegati superiori ai 30 MB.

È fatto divieto agli utenti di utilizzare lo strumento della posta elettronica per inviare, trasmettere o comunque divulgare a terzi non autorizzati informazioni riservate dell'Azienda.

In caso di assenza dal servizio dell'operatore per brevi periodi, è a disposizione apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

In caso di assenza non programmata, o dove non sia stata attivata la procedura di cui sopra, l'operatore può delegare altro operatore dell'ufficio a verificare il contenuto dei messaggi.

La consultazione via web della posta elettronica aziendale è possibile collegandosi al sito dell'Azienda e non necessita di autorizzazioni al primo accesso.

10. RETE TRASMISSIONE DATI E FONIA (WIRED e WIRELESS)

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive dell'ASST. In funzione di ciò viene fatto esplicito e tassativo divieto di collegare alla rete aziendale dispositivi informatici, se non dietro esplicita e formale autorizzazione dell'USC Informatica e telecomunicazioni. In ogni caso la configurazione di rete sarà effettuata da personale del USC IT o con i parametri standard. È altresì vietato alterare in qualsiasi modo la configurazione dei delle postazioni di lavoro (PDL)– o di altri dispositivi direttamente connessi alla rete, dati o fonia – per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati.

È assolutamente vietata l'installazione di Access Point personali.

11. PROTEZIONE DA VIRUS INFORMATICI

I Personal Computer aziendali sono dotati di un programma antivirus che avvia la scansione a scadenze ben definite a condizione che il Personal Computer risulti acceso e connesso alla rete aziendale; diversamente il programma antivirus si aggiorna automaticamente al primo avvio del Personal Computer.

Nel caso in cui il programma antivirus rilevi la presenza di un virus, l'operatore dovrà sospendere l'elaborazione in corso senza spegnere il computer, segnalando prontamente l'accaduto all'USC Informatica e telecomunicazioni.

Ogni dispositivo di memorizzazione (CD, DVD, floppy, chiavetta USB, disco esterno, ecc.) di provenienza esterna all'azienda verrà verificato dal programma antivirus prima di poter essere utilizzato.

12. CRIMINE INFORMATICO E TUTELE DEL DIRITTO D'AUTORE

I software utilizzabili sui Personal Computer aziendali sono solo ed esclusivamente quelli autorizzati dall'USC Informatica e telecomunicazioni.

È severamente vietato installare software di qualsiasi genere e da qualsiasi fonte senza l'autorizzazione da parte dell'USC Informatica e telecomunicazioni.

Vista la legge relativa alla tutela del diritto d'autore, si vieta la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi.

Si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del Titolare dei diritti esclusivi.

13. SMALTIMENTO DEI SUPPORTI DI MEMORIZZAZIONE

Secondo quanto disposto dal garante in materia di protezione dei dati personali i supporti contenenti dati devono essere smaltiti in modo da evitare il recupero di informazioni riservate.

I supporti rimovibili (DVD, CD, floppy, chiavette USB, dischi esterni) contenenti dati sensibili, se non utilizzati, devono essere distrutti o resi comunque inutilizzabili secondo quanto disposto dalla normativa vigente (Rifiuti di apparecchiature elettriche ed elettroniche – Raae - e misure di sicurezza dei dati personali). La dismissione dei dispositivi viene effettuata ad opera del personale dell'Help Desk aziendale in conformità al provvedimento sopra citato.

14. VERIFICHE

L'Azienda si riserva la facoltà di verificare, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito nell'uso degli strumenti elettronici, accesso a Internet e uso della posta elettronica.

Le verifiche si svolgeranno nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei lavoratori e dal Codice Privacy.

In particolare sarà possibile verificare gli accessi a Internet e i tempi di connessione senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal Codice Privacy.

A seguito delle verifiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.

Eventuali informazioni di natura sensibile - compreso il contenuto di e-mail trasmesse o ricevute dalle caselle di posta aziendale o l'elenco di siti oggetto di accesso - potranno essere trattate dall'Azienda a norma di legge.

Si sottolinea altresì che gli accessi ai dispositivi elettronici mediante la smartcard generano dei log che vengono registrati nei sistemi informatici presso l'USC Informatica e telecomunicazioni e conservati a tempo illimitato e che sono quindi accessibili nei modi previsti dalla legge.

15. SANZIONI

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, salve le azioni civili e penali consentite.

L'operatore è considerato direttamente responsabile per il danneggiamento della strumentazione informatica aziendale e delle relative infrastrutture, causato dall'uso improprio della stessa, salvo il diritto dell'Azienda di chiedere l'ulteriore risarcimento del danno. È altresì responsabile del trattamento illecito dei dati personali, ai sensi del D. Lgs. 196/2003, causato dall'uso improprio della smartcard aziendale, unico strumento che permette l'accesso sicuro e controllato alle applicazioni informatiche con le quali i dati vengono trattati.

16. RIFERIMENTI NORMATIVI E AZIENDALI

Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati personali)

Legge n.547 del 23/12/93 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"

LGIT03 "Linee guida per l'utilizzo delle cartelle condivise su server aziendali".

Legge. n. 248 del 18/8/2000 - "Nuove norme di tutela del diritto d'autore".

17. ALLEGATI

Allegato n.1 "Slocco_Cambio_PIN.pdf"

Manuale pratico per lo sblocco/cambio PIN della smartcard

Introduzione

I motivi per cui una smartcard (SISS oppure aziendale) si blocca sono, tipicamente, i seguenti:

- Blocco numerico attivato: si digitano dei numeri anziché delle lettere;
- Blocco maiuscolo attivato: si digitano i caratteri maiuscoli anziché quelli minuscoli;
- Non ci si ricorda più il PIN.

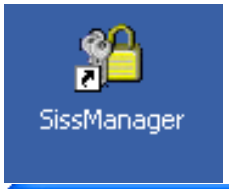
Se al momento della digitazione del PIN compare il messaggio "PIN errato" (o simili) occorre quindi porre particolare attenzione ai fattori descritti sopra.

Se il PIN viene digitato per 3 volte consecutive in modo errato, la smartcard viene bloccata.

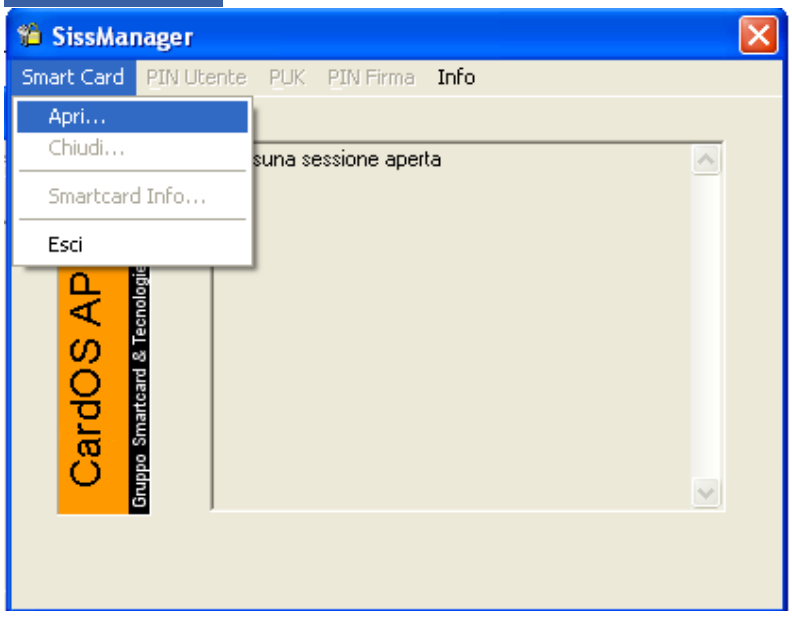
Per sbloccarla occorre avere sotto mano il PUK (PIN Unlock Key). Si consiglia di memorizzarlo in luogo sicuro ma accessibile al bisogno.

Modalità di sblocco PIN

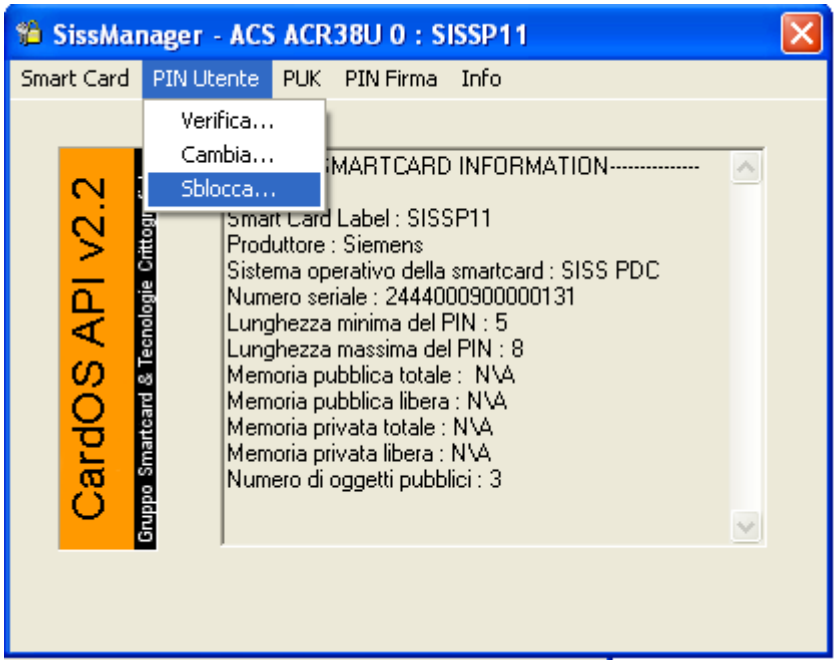
Inserire la carta nell'apposito lettore;
Dal menù start -> Programmi -> SISS selezionare la voce SISSManager, oppure cliccare sull'icona SISSManager presente sul Desktop;



Cliccare sulla voce di menù Smartcard -> Apri



Cliccare sulla voce di menù PIN utente -> Sblocca



Inserire il codice PUK nel primo campo, il codice PIN nel secondo e terzo campo (è possibile inserire anche lo stesso PIN utilizzato in precedenza) e cliccare sul tasto Sblocca;

Utilizzare il sistema nello stesso modo in cui si utilizzava prima del blocco della smartcard.

Modalità di cambio PIN

La procedura per il cambio PIN è simile a quella per lo sblocco (i punti 1, 2 e 3 sono identici), con la differenza che al punto 4 occorre selezionare la voce "Cambia" e al punto 5 occorre inserire il vecchio PIN nel primo campo in alto e il nuovo PIN (nei restanti due campi).