

# REGOLAMENTO IN MATERIA DI UTILIZZO DEI DISPOSITIVI INFORMATICI AZIENDALI ED ACCESSO ALLA RETE INTERNET

Deliberazione del Direttore Generale n. 16 del 24.01.2011

Premesse.....	3
Capo I – Principi generali .....	3
Art. 1 (Finalità) .....	3
Art. 2 (Principi applicabili).....	3
Art. 3 (Definizioni) .....	3
Capo II – Oggetto ed ambito di applicazione .....	4
Art. 4 (Oggetto).....	4
Art. 5 (Ambito di applicazione) .....	5
Capo III – Assegnazione dei dispositivi informatici e credenziali di accesso .....	5
Art. 6 (Assegnazione di un dispositivo informatico) .....	5
Art. 7 (consegna ed installazione dei dispositivi informatici nuovi).....	5
Art. 8 (Credenziali di accesso al sistema informatico) .....	6
Art. 9 (Accesso ai servizi informatici applicativi) .....	6
Art. 10 (Estinzione del rapporto contrattuale) .....	6
Capo IV – Uso dei dispositivi e servizi informatici aziendali .....	7
Art. 11 (Finalità) .....	7
Art. 12 (Utilizzo dei dispositivi informatici) .....	7
Art. 13 (Utilizzo di PC portatili) .....	7
Art. 14 (Uso dei dispositivi di archiviazione rimovibili) .....	8
Art. 15 (Utilizzo della rete fisica).....	8
Art. 16 (Utilizzo della rete logica).....	8
Art. 17 (Gestione delle credenziali di accesso).....	9
Art. 18 (Telefonia fissa e mobile).....	9
Art. 19 (Utilizzo di fax, fotocopiatrici e stampanti).....	10
Art. 20 (Tutela del diritto d'autore).....	10
Art. 21 (Manomissione dei dispositivi e della rete dati).....	11
Art. 22 (Facoltà dell'Azienda) .....	11
Art. 23 (Sanzioni) .....	11
Capo V – Navigazione nella rete Internet .....	11
Art. 24 (Usi consentiti).....	11
Art. 25 (Navigazione per fini non istituzionali).....	11
Art. 26 (Uso responsabile della rete Internet) .....	12
Art. 27 (Sanzioni) .....	12
Capo VI – Manutenzione e controlli .....	12
Art. 28 (Soggetti competenti) .....	12
Art. 29 (Manutenzione dei dispositivi informatici) .....	12
Art. 30 (Servizio di Assistenza) .....	13
Art. 31 (Infezione da virus informatici) .....	14
Art. 32 (Personale addetto ai controlli) .....	14
Art. 33 (Controlli a fini tecnici) .....	14
Art. 34 (Controlli preventivi).....	14
Art. 35 (Controlli successivi).....	15
Art. 36 (Controlli sulla navigazione in Internet) .....	15
Art. 37 (Procedimento disciplinare) .....	15
Art. 38 (Violazioni da parte del personale di controllo) .....	15
Art. 39 (Disposizioni finali e transitorie) .....	16
ALLEGATI .....	17
<b>Allegato A)</b> - Elenco attività di configurazione nuovo PC.....	17
<b>Allegato B)</b> Modulo richiesta credenziali accesso a Sistema Informatico .....	18
<b>Allegato C)</b> Modulo richiesta abilitazione accesso ai Sistema Informatici applicativi .....	19
<b>Allegato D)</b> Modulo richiesta riattivazione codici di accesso.....	20
<b>Allegato E)</b> Modulo richiesta di sostituzione o nuova attrezzatura informatica.....	21
<b>Allegato F)</b> Modulo richiesta di software .....	22
<b>Allegato G)</b> Modulo richiesta recupero dati .....	24
<b>Allegato H)</b> Modulo Consegna materiale informatico .....	25

<b>Allegato I)</b> Modulo scheda registrazione attività di assistenza e riparazione .....	26
---	----

## Premesse

L'Amministratore di sistema e i gestori delle applicazioni si adoperano per garantire, per quanto possibile, la massima fruibilità dei servizi applicativi minimizzando il rischio di usi impropri, quali:

- a) accessi non autorizzati ai dati
- b) usi impropri delle applicazioni che possano arrecare danno ad altri utenti del sistema, al sistema stesso o ad altri sistemi collegati alla rete Aziendale o a internet;
- c) usi illeciti dei dati o non attinenti alle attività istituzionali anche da parte degli utenti autorizzati.

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare l'accesso alla rete Internet dai Personal Computer, espone L'Azienda ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Azienda ha adottato un Regolamento atto ad evitare atteggiamenti non consoni che possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Tale regolamento si aggiunge ed integra le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Decreto Legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali).

## Capo I – Principi generali

### Art. 1 (Finalità)

Il presente regolamento è volto a disciplinare le modalità d'uso dei dispositivi informatici aziendali e l'accesso ad internet, stabilendo gli obblighi dell'utenza e dell'Azienda, nell'ottica di una più stretta e leale collaborazione nel rispetto delle reciproche attribuzioni.

### Art. 2 (Principi applicabili)

Il regolamento è redatto in conformità ai principi di cui all'art. 4 L.300/1970 , art. 3 ed 11 D.Lgs. 196/2003, nonché in applicazione della Deliberazione dell'Autorità Garante per la protezione dei dati personali n. 13 del 1 marzo 2007 e della Direttiva della Presidenza del Consiglio dei ministri n.2 del 2009.

I rapporti tra Azienda ULSS ed utenza si ispirano a principi di trasparenza e leale collaborazione.

### Art. 3 (Definizioni)

Ai fini del presente regolamento si intende per:

- a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite una rete di comunicazione elettronica;
- b) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- c) “posta elettronica”, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete di comunicazione elettronica, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;
- d) “dispositivi informatici”, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico, anche portatile, o comunque automatizzato con cui si fruisce dei servizi informatici aziendali;
- e) “servizi informatici aziendali”, l'insieme delle apparecchiature e delle risorse (ivi compresi i programmi per elaboratore, i dispositivi elettromedicali e gli apparati per l'accesso alla rete di comunicazione elettronica Internet) che consentono all'utente di accedere, visualizzare, modificare, e compiere ogni altra operazione su dati a qualunque titolo memorizzati nei dispositivi informatici aziendali, o da questi accessibili, nonché gli eventuali servizi ausiliari al loro funzionamento;
- f) “utente”, qualsiasi persona fisica che utilizza un servizio informatico aziendale;
- g) “responsabile di servizio”, il diretto superiore gerarchico dell'utente, come sopra definito, secondo le articolazioni previste dall'Atto Aziendale, ad esempio il Responsabile dell'Ufficio, il Direttore di Unità, il Direttore di Dipartimento, il Direttore di Struttura Tecnico Funzionale, il Direttore di Area, il Direttore Generale;
- h) “dati relativi al traffico”, qualsiasi dato sottoposto a trattamento riguardante la trasmissione di comunicazioni elettroniche e, anche alternativamente, l'uso di servizi di posta elettronica;
- i) “autenticazione informatica”, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- j) “credenziali di autenticazione”, i dati ed i dispositivi, in possesso di un utente, da questo conosciuti o ad esso univocamente correlati, utilizzati per l'autenticazione informatica;
- k) “parola chiave” o “password”, componente di una credenziale di autenticazione associata ad un utente ed a questo nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- l) “Amministratore del Sistema”, il responsabile del Servizio Informatico e gli incaricati da questo individuati;
- m) “Responsabile della Sicurezza” incaricato dal Direttore Generale di sorvegliare sulla sicurezza dei sistemi informatici (possibilmente non appartenente al Servizio Informatico)

Si applicano qualora compatibili le definizioni di cui all'art. 4 D.Lgs. 196/2003 non presenti nel comma precedente.

## **Capo II – Oggetto ed ambito di applicazione**

### **Art. 4 (Oggetto)**

Il presente regolamento disciplina le modalità d'uso dei dispositivi informatici aziendali in ogni aspetto, con riguardo sia all'utilizzo degli strumenti tecnologici, alla fruizione dei servizi informatici aziendali che alle regole comportamentali appropriate.

Sono altresì elencati gli obblighi dell'utente nei confronti dell'Azienda, dei colleghi e di altri soggetti destinatari di comunicazioni elettroniche.

Sono disciplinate modalità e finalità delle attività di controllo dell'impiego dei dispositivi, della manutenzione dei dispositivi informatici, della conservazione di registri contenenti dati relativi al traffico in ottemperanza ai dettami di cui all'art. 4 L. 300/1970.

Il presente regolamento costituisce regolamento disciplinare ai sensi dell'art. 7 L. 300/1970.

## **Art. 5 (Ambito di applicazione)**

Il regolamento si applica a tutti gli utenti che usufruiscono dei dispositivi informatici aziendali e dei servizi informatici aziendali, siano lavoratori dipendenti a tempo indeterminato o determinato oppure assunti con contratti di somministrazione, con contratto libero-professionale, collaboratori Co.Co.Co, specializzandi, borsisti, stagisti, Medici di M.G. e ad altri soggetti esplicitamente autorizzati dal responsabile della struttura di riferimento con il modulo **Allegato B**).

Il presente regolamento si applica altresì a chiunque acceda, anche a fini di manutenzione, a sistemi, dispositivi o servizi informatici aziendali.

Alla Direzione ed al personale che gestisce i dispositivi ed i servizi informatici aziendali e ne cura la manutenzione (Servizio Informatico), si applicano inoltre le disposizioni di cui al Capo VI del presente regolamento.

## **Capo III – Assegnazione dei dispositivi informatici e credenziali di accesso**

### **Art. 6 (Assegnazione di un dispositivo informatico)**

Qualora il lavoratore, per l'espletamento delle proprie mansioni, necessiti di un dispositivo informatico stabilmente assegnato, il Responsabile di Servizio formula la relativa richiesta nel modulo di cui all'**allegato E**. Analoga richiesta va formulata per la collocazione di dispositivi informatici ad uso promiscuo, in tal caso l'assegnatario è il Responsabile del Servizio medesimo.

Ogni richiesta è autorizzata dal Direttore di Area di riferimento.

Il Servizio informatico effettua un sopralluogo, concordato con il responsabile dell'U.O. richiedente, per verificare le condizioni per la collocazione dell'attrezzature quali:

- 1) presenza di un idoneo piano di supporto per collocare l'attrezzatura (spazio sul piano sufficiente, struttura di sostegno adeguata a sostenere il peso della attrezzatura, per gli schermi la disposizione rispetto alle finestre, ecc.) che risponda ai requisiti del Dlgs. 81/08
- 2) presenza di una presa di alimentazione elettrica in prossimità del luogo ove verrà collocata l'attrezzatura, altrimenti l'utente dovrà inoltrare apposita richiesta all'Ufficio Tecnico.
- 3) presenza di una presa a muro per allacciamento alla rete dati dell'edificio o di una rete wireless idonea; in caso contrario, l'operatore del Servizio Informatico aprirà una richiesta di ampliamento rete dati.
- 4) compatibilità con eventuali altre attrezzature informatiche che dovranno essere connesse all'apparecchiatura oggetto della richiesta (p. es. stampanti, scanner, lettori codici a barre ecc.).

Limitatamente all'assegnazione del dispositivo e compatibilmente con le scorte di magazzino, il Servizio informatico procede all'installazione entro 30 (trenta) giorni lavorativi dal ricevimento della richiesta.

### **Art. 7 (consegna ed installazione dei dispositivi informatici nuovi)**

Le attrezzature informatiche nuove sono consegnate ai richiedenti a cura del magazzino economale. Entro 10 (dieci) giorni lavorativi dalla consegna il Servizio Informatico effettua l'installazione, lo spostamento degli archivi informatici e l'eventuale ritiro dell'usato obsoleto. L'intervento è registrato sul modulo **Allegato I**) sottoscritto dal tecnico e dal dipendente presente durante l'intervento.

Con cadenza mensile il Servizio Informatico redige una lista delle attrezzature informatiche che sono state spostate da un ufficio all'altro e le trasmette all'U.O. Provveditorato per la registrazione dello spostamento sul registro dell'inventario.

Con cadenza semestrale il Servizio Informatico redige una lista delle attrezzature informatiche ritirate e in deposito perché guaste in modo irreparabile o certificate come obsolete e le trasmette all'U.O. Provveditorato per l'avvio della pratiche di dismissione.

### **Art. 8 (Credenziali di accesso al sistema informatico)**

Ai fini delle comunicazioni tra Azienda e lavoratore previste dalla normativa vigente, l'Azienda affida ad ogni dipendente le credenziali per l'accesso alle risorse di base del sistema informatico aziendale ed al sistema di posta elettronica.

Con riferimento alla costituzione di un nuovo rapporto di lavoro, l'U.O.C. Risorse Umane trasmette al Direttore dell'U.O.C. Servizio Informatico una richiesta di creazione ed attivazione delle credenziali di accesso al Sistema Informatico e della casella di posta elettronica aziendale nominativa tramite l'apposito modulo di richiesta, **allegato B)** al presente regolamento, debitamente compilato e sottoscritto per accettazione da parte del nuovo utente.

Il Servizio Informatico, entro tre giorni lavorativi dal ricevimento della richiesta, attiva l'account di dominio e la casella di posta elettronica aziendale e trasmette in busta chiusa al lavoratore per posta interna, le credenziali di accesso al sistema.

In caso di smarrimento della password l'utente interessato deve presentare una richiesta di ripristino al Servizio Informatico tramite il modulo **allegato D)**.

Il Servizio Informatico entro due giorni dalla ricezione della richiesta provvede a sostituire la password e ne trasmette copia all'interessato via posta interna in busta chiusa.

In entrambi i casi, sia che si tratti di consegna di nuove credenziali o di ripristino di una password perduta, l'utente è tenuto a modificare la password personale la prima volta che accede al sistema.

Il sistema di gestione delle credenziali forza gli utenti a sostituire la propria password personale ogni tre mesi, secondo quanto previsto dalla normativa T.U. 196/2003.

### **Art. 9 (Accesso ai servizi informatici applicativi)**

Qualora il lavoratore, per l'espletamento delle proprie mansioni, necessiti l'accesso ad uno o più servizi informatici aziendali o ad una o più cartelle delle unità di archiviazione comuni, il Responsabile di Servizio provvede ad inviare la richiesta di abilitazione all'U.O.C. Servizio Informatico, compilando il modulo all'**allegato C)** .

Il Servizio Informatico, entro tre giorni lavorativi dal ricevimento della richiesta, provvede a generare le credenziali di accesso all'eventuale sistema applicativo, comunicandole al lavoratore in busta chiusa via posta interna, oppure alla attribuzione dei diritti di accesso alle cartelle segnalate.

### **Art. 10 (Estinzione del rapporto contrattuale)**

In caso di estinzione del rapporto contrattuale con il lavoratore, l'UOC Risorse Umane ne dà tempestiva comunicazione, a mezzo posta elettronica, all'U.O.C. Servizio Informatico e questi provvede ad inibire l'accesso ai servizi informatici aziendali entro tre giorni lavorativi dal ricevimento della comunicazione.

Entro i dieci giorni lavorativi successivi, il Servizio informatico procede con il recupero dei dispositivi informatici precedentemente assegnati al lavoratore, prendendo accordi con il Responsabile di Servizio per la migrazione dei dati ivi eventualmente contenuti.

In ogni caso il Servizio informatico procede con la formattazione del dispositivo informatico e sua riconfigurazione.

## **Capo IV – Uso dei dispositivi e servizi informatici aziendali**

### **Art. 11 (Finalità)**

L'uso dei dispositivi e dei servizi informatici aziendali è concesso esclusivamente per l'espletamento delle mansioni lavorative, nell'ambito dell'attività di servizio o dell'attività libero-professionale intramuraria.

È altresì concesso qualora sia indispensabile per il regolare svolgimento di un rapporto contrattuale corrente con l'Azienda sanitaria.

I dispositivi informatici assegnati hanno carattere aziendale, escluso ogni uso personale, e possono essere soggetti a controllo, anche nei contenuti, da parte del Responsabile di Servizio.

È esclusa la natura riservata o confidenziale dei dati memorizzati nei dispositivi assegnati agli utenti, immessi nei servizi informatici aziendali o comunque comunicati attraverso l'infrastruttura tecnologica aziendale.

### **Art. 12 (Utilizzo dei dispositivi informatici)**

L'accesso ai PC è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete e per l'accesso a qualsiasi applicazione. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dei Sistemi Informativi.

Non è consentito installare o rimuovere autonomamente programmi, salvo esplicita autorizzazione dell'Amministratore del Sistema, a causa del grave pericolo di introdurre Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito all'utente modificare la configurazione pre-impostata dei dispositivi informatici, salvo esplicita autorizzazione dell'Amministratore del Sistema.

Il Personal Computer deve essere spento o bloccato ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete con il proprio utente e password inseriti può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...), se non con l'autorizzazione esplicita ed il supporto dell'Amministratore del Sistema.

Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più postazioni informatiche.

### **Art. 13 (Utilizzo di PC portatili)**

L'utente è responsabile del Personal Computer portatile Aziendale assegnatogli temporaneamente dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Il PC portatile non deve mai essere lasciato incustodito né in luoghi aperti al pubblico né in automobile. I PC portatili Aziendali utilizzati all'esterno (convegni, visite in Azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Il PC portatile utilizzato in ufficio deve essere chiuso in armadio sotto chiave quando il titolare è assente e nelle ore di chiusura dell'ufficio.

L'utente dovrà collegarsi periodicamente alla rete interna per consentire il caricamento degli aggiornamenti.

Nell'utilizzo del dispositivo informatico, si attiene alle prescrizioni di sicurezza ricevute dal Responsabile del trattamento dei dati personali.

Ai PC portatili aziendali si applicano le regole di utilizzo previste per i PC connessi in rete.

#### **Art. 14 (Uso dei dispositivi di archiviazione rimovibili)**

L'uso di dispositivi di archiviazione dati rimovibili (ad esempio CD-ROM, chiavette USB, hard-disk portatili) è vietato.

Qualora fosse ravvisata la necessità di impiegare tali dispositivi, il Responsabile di Servizio interessato presenta richiesta motivata al Direttore dell'U.O.C. Servizio Informatico. Questi ne valuta l'impatto sulla sicurezza dei dispositivi informatici, sui servizi aziendali e sull'integrità e la sicurezza dei dati e riscontra la richiesta entro cinque giorni lavorativi dal ricevimento.

In caso di accoglimento, il Servizio informatico fornisce le indicazioni e gli eventuali dispositivi e/o supporti necessari per garantire la sicurezza dei sistemi informatici aziendali e degli eventuali dati sensibili nonché informazioni costituenti know-how aziendale.

Si intende vietato anche il collegamento ai dispositivi informatici aziendali di telefoni cellulari, PDA, lettori MP3, escluso il caso di collegamento finalizzato alla sincronizzazione delle agende e/o rubriche elettroniche.

#### **Art. 15 (Utilizzo della rete fisica)**

La rete di trasmissione dati e fonia è una risorsa strategica per l'Azienda in quanto connette ogni dispositivo informatico veicolando i dati conservati negli archivi centrali, inoltre, funge da mezzo di trasporto per altri tipi di informazioni (ad esempio, telefonia interna, videoconferenza, formazione a distanza, telemedicina, telecontrollo degli apparati) pertanto ogni disservizio o sua interruzione comporta notevoli disagi per l'operatività dell'Azienda medesima.

Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico se non dietro esplicita e formale autorizzazione dell'U.O.C. Servizio Informatico. Preliminarmente al collegamento alla rete dati aziendale, ogni dispositivo informatico deve essere configurato secondo quanto previsto dall'apposita "Check List", di cui all'**allegato A**), che elenca i software da installare e le configurazioni da applicare .

E' proibito a chiunque l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto.

E' vietato depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.

E' vietato calpestare o schiacciare con arredi, sedie ecc., i cavi di collegamento della rete alle postazioni.

E' obbligatorio interpellare l'U.O. Sistemi Informativi prima di ogni spostamento di postazioni informatiche, per valutarne l'impatto e la fattibilità e per predisporre le configurazioni adeguate.

#### **Art. 16 (Utilizzo della rete logica)**

Le unità di archiviazione di rete presenti sul server possono essere comuni a gruppi omogenei di lavoro o strettamente personali e non visibili ad altri utenti: a cura dell'utilizzatore può essere richiesta l'eventuale modifica alla visibilità da parte degli altri utenti.

E' vietato condividere localmente dischi, cartelle o risorse (es. cartelle di scambi) ad eccezione delle stampanti comuni. Per le esigenze di scambio di file tra uffici sono disponibili strutture adeguate presso i server dell'U.O. Sistemi Informativi.

E' vietata l'archiviazione di uno stesso file in posizioni differenti delle unità di archiviazione di rete.

## **Art. 17 (Gestione delle credenziali di accesso)**

Al primo accesso l'utente deve provvedere a modificare la password personale fornita dal Servizio Informatico.

E' proibito accedere alle postazioni informatiche, alla rete ed ai programmi con credenziali altrui.

La password, formata da lettere (maiuscole o minuscole hanno significato diverso) e/o numeri anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

E' obbligatoria la sostituzione immediata della propria password personale ogniqualvolta abbia perso la segretezza o l'utente sospetti possa essere stata utilizzata da terzi. In tal caso, ne deve dare comunicazione all'Amministratore del Sistema.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla persona stessa o all' Amministratore del Sistema.

Soggetto preposto alla custodia delle credenziali di autenticazione di sistema (Admins o Administrators) è l'Amministratore del Sistema e gli incaricati da questo individuati. L'Amministratore di sistema ha l'obbligo di sostituire le password di default o di installazione che non devono in nessun caso essere utilizzate nel corso dell'esercizio del sistema informatico.

Qualora il prodotto utilizzato renda impossibile la definizione di password personali, deve essere tenuta traccia degli accessi al sistema mediante registrazione degli stessi in un apposito registro cartaceo.

Ciascun Amministratore di Sistema registrerà le password da lui utilizzate in un foglio che sarà inserito in una busta chiusa da lui siglata. Le buste saranno conservate in un luogo protetto ma accessibile in condizioni di emergenza. Le password, e le relative buste, dovranno essere modificate con periodicità commisurata alla criticità degli ambienti e comunque non superiore al trimestre.

Le buste potranno essere aperte, previa autorizzazione del Responsabile della Sicurezza (custode password), nei seguenti casi:

- necessità urgente di intervento su un sistema in assenza dei relativi Amministratori;
- dimenticanza della password da parte dell'Amministratore di Sistema;

In entrambi i casi gli Amministratori di Sistema dovranno definire nuove password e ricreare la busta.

Qualora si verifichi una condizione di emergenza che richieda l'apertura urgente delle buste per l'accesso ai sistemi e non sia possibile ottenere l'autorizzazione da parte del Responsabile della Sicurezza (o da persona da questi delegata), l'Amministratore di Sistema potrà agire in deroga a tale autorizzazione redigendo contestualmente un documento probatorio firmato.

## **Art. 18 (Telefonia fissa e mobile)**

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa

stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

L'Azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri – ad esempio numeri a pagamento per servizi particolari che si giudicano non interessanti dal punto di vista istituzionale, ecc..., l'operatore che abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione.

Qualora venisse assegnato un cellulare aziendale all'utente, si applica il "regolamento per l'utilizzo di apparecchi telefonici cellulari di servizio".

Per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate qualora queste inducano un onere economico per l'Azienda registrando:

- il numero del chiamante;
- il numero chiamato;
- la data e ora di inizio della telefonata e la data e ora di fine della stessa

Tutti i log sopra citati vengono conservati dall'Azienda per un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti. I dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi.

I controlli verranno effettuati in maniera non nominativa ed aggregata (ad esempio aggregando i dati per edificio o per unità erogante). Qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi potranno essere ulteriormente approfonditi prevedendo una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati.

Qualora l'integrità del sistema tecnologico dell'azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato.

Qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione. Tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda.

Qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative.

### **Art. 19 (Utilizzo di fax, fotocopiatrici e stampanti)**

È vietato l'utilizzo per fini personali dei fotocopiatori aziendali e dei fax aziendali, tanto per spedire quanto per ricevere documentazione.

L'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.

### **Art. 20 (Tutela del diritto d'autore)**

Con riferimento alla L. n. 633 del 22.04.1941 – "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio", 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.

E' fatto divieto ad ogni utilizzatore del sistema informativo aziendale di scaricare, gestire o in qualsiasi modo trattare dati o informazioni che violino la normativa sulla tutela del diritto d'autore.

Qualora l'operatore nonostante tale divieto infranga tale normativa sarà penalmente e civilmente responsabile del proprio operato sollevando l'azienda da ogni responsabilità.

### **Art. 21 (Manomissione dei dispositivi e della rete dati)**

È vietata ogni attività volta a danneggiare, accedere abusivamente o rendere non accessibili i servizi informatici aziendali.

### **Art. 22 (Facoltà dell'Azienda)**

In caso di problemi inerenti la sicurezza, a seguito del riscontro di anomalie o malfunzionamenti dell'infrastruttura tecnologica, l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza.

L'Azienda si riserva la facoltà di sospendere l'accesso ai servizi in caso di inadempienze al presente Regolamento da parte dell'operatore.

L'Azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia ad avvertire preventivamente gli utenti.

Il Servizio deputato ai controlli previsti dal presente Regolamento è l'U.O.C. Servizio Informatico.

### **Art. 23 (Sanzioni)**

La violazione delle prescrizioni di cui agli articoli precedenti di questo Capo, costituisce illecito disciplinare valutabile ai sensi dell'art. 28 C.C.N.L. 1 settembre 1995 e successive modifiche per il personale del Comparto, dell'art. 6 C.C.N.L. 6 maggio 2010 e successive modifiche per la Dirigenza S.P.T.A. e dell'art. 6 C.C.N.L. 6 maggio 2010 e successive modifiche per Dirigenza Medica e Veterinaria e del Regolamento Disciplinare Aziendale per tutte le categorie di utenti. Sono salvi eventuali ulteriori risvolti civili e penali.

Relativamente al personale non dipendente la violazione di cui agli articoli precedenti potrà determinare il blocco delle credenziali di accesso e, in casi di particolare gravità, l'illecito potrà costituire giusta causa di recesso dal rapporto contrattuale.

## **Capo V – Navigazione nella rete Internet**

### **Art. 24 (Usi consentiti)**

È escluso l'impiego a fini non istituzionali della rete Internet, salve le eccezioni indicate all'articolo seguente.

### **Art. 25 (Navigazione per fini non istituzionali)**

È consentita, nei limiti di tempo strettamente necessari e per un periodo comunque non superiore ai 30 minuti giornalieri, la navigazione nella rete Internet per assolvere incombenze amministrative e/o burocratiche.

Si intendono, per incombenze di cui al comma precedente, adempimenti on-line nei confronti di pubbliche amministrazioni, concessionari di servizi pubblici, istituti bancari e assicurativi. I casi di deroga al divieto generale di impiego della rete Internet a fini non istituzionali, individuati al presente articolo, sono tassativi.

### **Art. 26 (Uso responsabile della rete Internet)**

L'utente deve, ove possibile, evitare di scaricare file di dimensioni superiori ai tre megabyte, al fine di non compromettere la disponibilità di risorse condivise con il restante personale dell'Azienda.

In ogni caso, salvo le deroghe per il personale di cui all'art. 29 (*Manutenzione dei dispositivi informatici*), è vietato scaricare programmi non autorizzati dall'Azienda.

Qualora i filtri automatici di cui all'art. 36 dovessero bloccare siti internet di utilità per l'Azienda il Dirigente Responsabile dell'U.O. interessata inoltra segnalazione al Direttore dell'U.O. Servizio Informatico e questi provvederà ad inserire il sito richiesto nella cosiddetta "white list"

### **Art. 27 (Sanzioni)**

La violazione delle prescrizioni di cui agli art. 24 (*Usi consentiti*) e art. 25 (*Navigazione per fini non istituzionali*), costituisce illecito disciplinare valutabile ai sensi dell'art. 28 C.C.N.L. 1 settembre 1995 e successive modifiche per il personale del Comparto, dell'art. 35 C.C.N.L. 5 dicembre 1996 e successive modifiche per la Dirigenza S.P.T.A. e dell'art. 36 C.C.N.L. 5 dicembre 1996 e successive modifiche per Dirigenza Medica e Veterinaria e del Regolamento Disciplinare Aziendale per tutte le categorie di utenti. Sono salvi eventuali ulteriori risvolti civili e penali.

Relativamente al personale non dipendente la violazione di cui agli articoli precedenti potrà determinare il blocco delle credenziali di accesso e, in casi di particolare gravità, l'illecito potrà costituire giusta causa di recesso dal rapporto contrattuale.

## **Capo VI – Manutenzione e controlli**

### **Art. 28 (Soggetti competenti)**

Competente all'effettuazione delle attività di manutenzione, controllo e verifica, è l'U.O.C. Servizio informatico.

Il personale preposto all'U.O.C. Servizio Informatico esegue le attività di cui al comma precedente nei limiti del proprio ambito tecnico di competenza.

### **Art. 29 (Manutenzione dei dispositivi informatici)**

La manutenzione dei dispositivi informatici aziendali è effettuata, ove possibile, in via telematica. I dispositivi sono configurati di modo che il personale di cui all'art. 28 (*Soggetti competenti*) possa, su richiesta dell'utente, intervenire tempestivamente.

Per i fini di cui al comma precedente, sui dispositivi informatici aziendali è installato un *server VNC* configurato di modo che l'utente sia consapevole dell'intervento del personale tecnico. La durata del collegamento è limitata al tempo strettamente necessario per l'esecuzione e la verifica dell'intervento effettuato.

Nel caso in cui l'intervento in via telematica appaia o si riveli inefficace, il Servizio informatico provvede ad operare direttamente presso la sede ove si trova il dispositivo informatico mal funzionante.

L'Amministratore del Sistema per l'espletamento delle sue funzioni (p. es. salvataggio e ripristino di archivi, tutela della sicurezza informatica), ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica.

L'amministratore del Sistema può in qualunque momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza sia sulle postazioni informatiche degli incaricati sia sulle unità a dischi di rete.

### **Art. 30 (Servizio di Assistenza)**

Il Servizio informatico adotta, attraverso il personale a ciò preposto, tutti gli accorgimenti necessari per garantire il corretto funzionamento dei dispositivi e servizi informatici aziendali.

Ogni richiesta di riparazione, supporto o consulenza informatica deve essere attivata, tramite telefono o via e-mail, presso il servizio di "Help Desk" Informatico, preposto alla gestione dell'iter degli interventi e della relativa programmazione.

Il servizio di supporto ed assistenza interessa ogni possibile interazione con gli strumenti informatici presenti in azienda, ed in particolare:

- Utilizzo dei personal computer e programmi ivi installati;
- Periferiche di stampa;
- Apparati telefonici;
- Posta Elettronica, Intranet ed accesso ad Internet;
- Rete dati aziendale.

Sono esclusi dal servizio di assistenza e supporto:

- Acquisto o sostituzione di attrezzature informatiche, per le quali occorre presentare richiesta su apposito modulo **allegato E**).
- Materiale di consumo (toner, carta per stampanti), di pertinenza dell'U.O.C. Provveditorato.
- Modifiche agli Impianti elettrici o alla configurazione delle centrali telefoniche, di pertinenza dell'U.O. Ufficio Tecnico;
- Manutenzione FAX e Fotocopiatori, di pertinenza dell'U.O.C. Provveditorato.

Sono inoltre esclusi i sistemi od impianti la cui gestione è in carico al fornitore o per i quali è stato attivato un contratto di manutenzione specifico che prevede l'accesso diretto al servizio di assistenza specialistico da parte degli utenti finali, al fine di velocizzare la soluzione dei problemi, ed in particolare:

- Stampanti Fuji per la produzione di immagini radiologiche sulle stampanti è indicato direttamente il numero del supporto assistenza;
- Stampanti/Fax Xerox di reparto (Assistenza Clienti, Amministrazione e Direzione): sulle stampanti è indicato direttamente il numero del supporto assistenza;
- Robot per la masterizzazione in serie dei CD-ROM paziente.

In nessun caso eventuali ritardi nelle mansioni lavorative dovuti a malfunzionamento dei dispositivi o dei servizi saranno addebitabili all'utente, salvo quanto previsto all'art. 17 (*Credenziali di accesso*), all'art. 21 (*Manomissione dei dispositivi e della rete dati*), all'art. 14 (*Uso dei dispositivi di archiviazione rimovibili*) e salvi i casi di dolo o colpa grave.

### **Art. 31 (Infezione da virus informatici)**

Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato da virus informatico si deve avvertire tempestivamente il servizio di assistenza informatica e non effettuare alcuno scambio di dati con altri.

Solo l'U.O.C Servizio Informatico è autorizzato a diffondere messaggi di allerta a fronte di eventuali attacchi virali.

L'infezione da virus informatici avvenuta in seguito alla navigazione nella rete Internet ed i conseguenti danni non sono addebitabili all'utente, salvo la violazione delle disposizioni di cui all'art. 24 (*Usi consentiti*) e art. 26 (*Uso responsabile della rete Internet*).

Ferma la responsabilità disciplinare, l'utente assume ogni più ampia responsabilità per l'infezione da virus informatici, e conseguenti danni, avvenuta in occasione dell'impiego non autorizzato dei dispositivi di cui all'art. 14 (*Uso dei dispositivi di archiviazione rimovibili*).

### **Art. 32 (Personale addetto ai controlli)**

L'Azienda individua il personale addetto ai controlli sull'uso dei dispositivi e dei servizi informatici aziendali (ivi compresa la navigazione nella rete Internet), da effettuarsi nei termini indicati negli articoli seguenti, nel personale in organico presso l'U.O. Servizio Informatico.

Detto personale è tenuto al riserbo ed al rispetto dei principi enunciati negli articoli seguenti.

La violazione delle disposizioni di cui al comma precedente costituisce illecito disciplinare, valutabile ai sensi dell'art. 28 C.C.N.L. 1 settembre 1995 e successive modifiche per il personale del Comparto, dell'art. 35 C.C.N.L. 5 dicembre 1996 e successive modifiche per la Dirigenza Tecnica, del Regolamento Disciplinare Aziendale e dell'art. 167 D.Lgs. 196/2003 per entrambe le categorie. Sono salvi eventuali ulteriori risvolti civili e penali.

È fatta salva la possibilità, da parte del Responsabile di Servizio, di procedere a controlli ispettivi sui dati e sui contenuti delle comunicazioni elettroniche degli utenti, anche in loro assenza, qualora se ne ravvisi la necessità ai fini di procedimenti disciplinari.

### **Art. 33 (Controlli a fini tecnici)**

Al fine di provvedere alle necessarie incombenze di natura tecnica, l'Azienda effettua una temporanea registrazione dei dati relativi all'uso dei servizi informatici aziendali. In particolare tali controlli sono finalizzati a:

- verificare il corretto funzionamento dei servizi;
- individuare in tempi rapidi eventuali malfunzionamenti ed approntare una soluzione;
- effettuare interventi di manutenzione periodica;
- vigilare sulla sicurezza dei servizi ed in generale dei sistemi informatici aziendali.

I *software* sono configurati in modo tale da eliminare periodicamente e in modo automatico, al riempimento dello spazio di memorizzazione a tale scopo dedicato, le registrazioni di cui al primo comma; in ogni caso le registrazioni si conformano ai principi di necessità, pertinenza e non eccedenza.

### **Art. 34 (Controlli preventivi)**

L'Azienda può effettuare controlli preventivi diretti a verificare il rispetto delle disposizioni del presente regolamento, esclusivamente mediante l'analisi statistica e anonima dei dati relativi al traffico telematico ed all'uso dei servizi.

I controlli di cui al comma precedente si conformano ai principi di necessità, pertinenza e non eccedenza e le relative registrazioni sono eliminate periodicamente e in modo automatico, al riempimento dello spazio di memorizzazione a tale scopo dedicato.

### **Art. 35 (Controlli successivi)**

Su segnalazione del Responsabile di U.O., in sede di accertamento disciplinare, l'Azienda può eseguire controlli sui dati relativi al traffico, sui contenuti delle comunicazioni elettroniche, sui dati memorizzati dall'utente, memorizzati sul dispositivo informatico ad egli assegnato o sui sistemi centrali, necessari alla definizione della controversia. In tal caso, le registrazioni dei controlli effettuati saranno conservate fino all'avvenuta definizione della controversia stessa.

### **Art. 36 (Controlli sulla navigazione in Internet)**

L'Azienda regola la navigazione nella rete Internet attraverso l'implementazione di *black lists* che inibiscono, preventivamente, l'accesso a siti dal contenuto chiaramente non attinente alle attività istituzionali, contrario al buon costume, potenzialmente pericoloso per la sicurezza e l'integrità dei dispositivi e servizi informatici aziendali.

L'Azienda può implementare sistemi di ripartizione del traffico telematico che, nell'ottica di garantire una migliore fruizione del servizio alla generalità del personale, privilegino l'accesso a siti il cui contenuto sia valutato di maggiore rilevanza per i fini aziendali.

Sull'impiego del servizio di accesso alla rete Internet vengono effettuati i controlli di cui agli art. 33 (*Controlli a fini tecnici*) e art. 34 (*Controlli preventivi*).

Nel caso in cui il personale ispettivo riscontri anomalie o violazioni degli art. 24 (*Usi consentiti*) e art. 25 (*navigazione per fini non istituzionali*) il Direttore del Servizio informatico pubblica un avviso sul sito intranet aziendale, con il quale invita gli utenti, individuati per aggregazioni rispondenti alla sede da cui sono state registrate le anomalie o le violazioni, a desistere dalla condotta censurata.

Nel caso in cui le violazioni persistano, il Servizio informatico adotta le misure opportune per individuare l'utente ed assicurare il rispetto della presente disciplina.

In caso di grave pericolo per la sicurezza dei servizi informatici, per la sicurezza o l'integrità dei dati o dei dispositivi informatici aziendali, il Direttore del Servizio informatico può adottare provvisoriamente le misure ritenute necessarie per impedire il danno.

Nei casi di cui ai due commi precedenti il Direttore del Servizio Informatico dà tempestiva segnalazione delle anomalie o violazioni riscontrate al Responsabile di Servizio dell'utente.

### **Art. 37 (Procedimento disciplinare)**

In seguito all'accertamento di violazioni del presente regolamento perpetrate dall'utente, acquisito parere scritto da parte del Direttore del Servizio Informatico e svolti, se necessario, i controlli di cui all'art. 35 (*controlli successivi*), il procedimento si svolge secondo quanto previsto dal Regolamento Disciplinare Aziendale.

### **Art. 38 (Violazioni da parte del personale di controllo)**

Gli art. 14 (*uso dispositivi di archiviazione rimovibili*), art. 17 (*gestione delle password*), art. 26 (*Uso responsabile della rete Internet*) e art. 37 (*Procedimento disciplinare*) si applicano anche al personale di cui all'art. 28 (*Soggetti competenti*).

### **Art. 39 (Disposizioni finali e transitorie)**

Entro 45 giorni dall'entrata in vigore del presente Regolamento, tutti gli utenti sono tenuti a rimuovere dai dispositivi aziendali in loro utilizzo eventuali dati di carattere non aziendale.

Entro lo stesso termine gli utenti dovranno richiedere la disinstallazione di eventuali programmi informatici installati senza la prevista autorizzazione da parte del Servizio Informatico.

# ALLEGATI

**Allegato A)** - Elenco attività di configurazione nuovo PC

## CHECK LIST PREPARAZIONE PERSONAL COMPUTER

Tutti i personal computer, sia stazioni di lavoro individuali o di uso promiscuo, di proprietà dell'azienda o di fornitori esterni (anche solo temporaneamente collegati alla rete dati aziendale), dispositivi di interfacciamento ad attrezzature elettromedicali o di analisi, o elaboratori inglobati in dispositivi elettromedicali medesimi **devono tassativamente esser predisposti** secondo le seguenti specifiche tecniche:

- 1) **I programmi eventualmente forniti** devono poter operare con un utenti di tipo **"Users"**;
- 2) Scaricare ed installare tutte le patch e fix del sistema operativo;
- 3) Attribuire un indirizzo IP statico fornito dal Servizio di assistenza e coerente con gli standard aziendale di attribuzione degli indirizzi IP;
- 4) Attribuire un identificativo che rispetti la seguente indicazione: XXXYYYNN dove:
  - a. XXX è un acronimo che rappresenta il reparto/servizio a cui appartiene il personal computer (CAR cardiologia, RAD radiologia, MED medicina, DIS distretto);
  - b. YYY è un acronimo che rappresenta la sede in cui è collocato il PC (ARZ Arzignano, MON Montecchio, LON Lonigo, VAL Valdagno, ecc.)
  - c. ZZ un numero incrementale a partire da 01 che individua univocamente il PC tra gli altri presente nello stesso reparto/servizio;
- 5) Eliminare tutte le condivisioni predefinite da Microsoft (ove non siano indispensabili), in particolare C\$, D\$, WINNT\$, ADMIN\$ etc. (si può anche disabilitare via registry l'autoshare server e utilizzando un "restrict anonymous access");
- 6) Qualora fosse indispensabile mantenere alcune condivisioni autorizzare solamente alcuni utenti possibilmente non locali ma di dominio aziendale Active Directory
- 7) Creare un utente amministratore ad uso esclusivo del servizio informatico nominato sil-amminisbxc bdf dfbd b tratore con password "....." (non eliminare l'account "Administrator" ed inserire la medesima password di "sil-amministratore").
- 8) Creare uno o più utenti di tipo "Administrators", ad uso esclusivo della ditta fornitrice concordando con la medesima la password correlata.
- 9) Disabilitare gli utenti utenti di tipo "Guests";
- 10) Installare il software di controllo remoto UltraVNC e configurarlo come servizio automatico con le seguenti opzioni:
  - a. Autenticazione via MS-Logon;
  - b. Attivare finestra popup di autorizzazione alla connessione;
  - c. Eliminare lo sfondo.
- 11) Verificare che il browser di tipo "MS Internet Explorer" sia nella versione 6.0 sp1 comprensiva di tutte le successive patches di aggiornamento e protezione1.
- 12) Sono autorizzati PC con Licenza Windows 7 Professional o Windows XP Professional, ma è esclusa la fornitura di licenze di Windows Vista. In ogni caso devono essere installate tutte le successive patches di aggiornamento e protezione.
- 13) Installare i programmi di utilità quali: Acrobat Reader, un compressore (preferibilmente 7-zip in italiano), java virtual machine.
- 14) Installare l'Antivirus Aziendale in accordo con il Servizio Informatico, solo quando il PC è in rete aziendale;
- 15) Installare Citrix ICA Client;
- 16) Sulle postazioni utilizzabili dagli utenti anche per svolgere altre funzioni entrare con il profilo di amministratore locale nei seguenti siti per caricare gli ActiveX o OCX associati:
  - a. Laboratorio Analisi -> tentare la stampa di una etichetta.
  - b. Protocollo Informatico -> attivare il sistema ed aprire la "scrivania"

**Allegato B)** Modulo richiesta credenziali accesso a Sistema Informatico



Data .....

Alla c.a.  
**Ufficio Sistemi Centrali e Sicurezza**  
**U.O.C. SERVIZIO INFORMATICO**  
v. Trento 4, 36071 Arzignano (VI)

Oggetto: richiesta attivazione credenziali di  
accesso al sistema informatico

Il sottoscritto .....

In possesso del codice fiscale .....

assunto/collaboratore presso l'U.O. ....  
(servizio/reparto e sede lavorativa)

in servizio dalla data ..... / ..... / .....

**INFORMATO CHE:**

l'Azienda ULSS n. 5 affida ad ogni dipendente o collaboratore i codici personali di accesso al Sistema Informatico Aziendale (Dominio Sanita/Citrix) ed una Casella di Posta Elettronica personale.

**DICHIARA**

inoltre di essere a conoscenza che:

1. i codici di accesso sono elementi fondamentali per la sicurezza del sistema informatico aziendale, pertanto, sono strettamente personali e sarà necessario porre la massima attenzione affinché rimangano di propria esclusiva conoscenza;
2. è assolutamente vietato portare a conoscenza di terzi, sia colleghi che estranei all'azienda, i codici di accesso personali e la loro trascrizione su qualsiasi supporto, accessibile a terzi.
3. è vietato trascrivere la password su biglietti, documenti o altro accessibili a terzi.
4. il sottoscritto sarà ritenuto personalmente responsabile degli eventuali danni od abusi al sistema informatico compiuti da terzi venuti in possesso dei codici personali;
5. L'impiego dei sistemi informatici aziendali è sottoposto alla vigilanza del Servizio informatico. Eventuali abusi potranno essere segnalati al responsabile di servizio.
6. In caso di perdita o dimenticanza della password personale ci si dovrà rivolgere al Servizio Informatico per la riattivazione.

Per qualsiasi informazione è a disposizione il servizio Informatico 0444 459555.

.....  
(firma)

**Allegato C)** Modulo richiesta abilitazione accesso ai Sistema Informatici applicativi



Alla c.a.  
**Ufficio Sistemi Centrali e Sicurezza**  
**U.O.C. SERVIZIO INFORMATICO**  
Via Trento 4 - 36071 Arzignano

Oggetto: **richiesta codici d'accesso**

Il sottoscritto, .....,  
responsabile dell'U.O. .... con sede a .....,  
(servizio/reparto)  
tel. num.: .....

**CHIEDE:**

L'attivazione delle credenziali di accesso per i seguenti programmi informatici:

.....  
.....  
.....

Il recupero, causa   mancato rinnovo /   dimenticanza, della password per il programma:.....

per le seguenti persone:

<b>Nome e Cognome</b>	<b>Codice Fiscale (obbligatorio)</b>
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

accompagnando alla presente i fogli informativi, firmati (*superflui se la password va solo rinnovata*) da ognuno dei suddetti o con l'impegno di farli avere entro 3 giorni lavorativi.

Distinti saluti.

Data, .....

**IL RESPONSABILE**

.....



Alla c.a.  
**Ufficio Sistemi Centrali e Sicurezza**  
**U.O.C. SERVIZIO INFORMATICO**  
Via Trento 4 - 36071 Arzignano

Oggetto: **richiesta rinnovo codici d'accesso**

Il sottoscritto, .....

in servizio presso l'U.O. ....  
(servizio/reparto)

con sede in .....  
(indirizzo a cui spedire le credenziali)

tel. num.: .....

**DICHIARA:**

di non essere più in possesso delle credenziali di accesso ai seguenti sistemi informatici:

- .....
- .....
- .....
- .....

a causa   scadenza periodo validità -  dimenticanza  
pertanto

**CHIEDE**

la riattivazione

Distinti saluti.

Data, .....

.....  
(firma)

**- Servizio Informatico -**

**Modulo presentazione richieste attrezzature informatiche e collegamento rete dati**

(compilare una scheda per ogni postazione(PC+video)/stampante/accessorio/richiesta di collegamento richiesti)

C.d.C.: _____ <small>Centro di costo</small>	Descrizione: _____ <small>U.O.A. / Servizio / Ufficio</small>	
Utente: _____ <small>Cognome e nome di chi utilizzerà il/i bene/i richiesto/i</small>	Telefono: _____ <small>Recapito telefonico per consegna</small>	
Collocazione: _____ <small>Sede</small>	_____ <small>Piano</small>	_____ <small>Ufficio</small>

**Bene richiesto**

**Sostituisce (compilare solo se richiesta sostituzione):**

PC/Terminale	Inventario: _____	Marca/modello _____
Monitor	Inventario: _____	Marca/modello _____
Stampante	Inventario: _____	Marca/modello _____
Scanner	Inventario: _____	Marca/modello _____
Accessori	_____ <small>Descrizione dell'accessorio</small>	
collegamento rete dati	Numero prese n.: _____ * Compilazione riservata al personale del Servizio Informatico	
<small>* barrare solo se non è presente una presa di rete dati libera</small>		
Cavo di rete	Lunghezza m.: _____	
<small>* barrare se è si tratta di postazione nuova o se il cavo attuale è corto</small>		
Ciabatta elettrica a norma	<small>barrare se il numero delle prese elettriche a muro è insufficiente oppure se le prese a muro sono lontane dalla postazione oppure se la ciabatta elettrica attuale non è dotata di interruttore e fusibile</small>	
<small>* Compilazione riservata al personale del Servizio Informatico</small>		
Lunghezza cavo: m. _____	Tipo presa a muro: _____	Numero prese: _____
Tipo fissaggio: _____	Lunghezza canalina: m. _____ muro/pavimento	

Motivazione della richiesta e destinazione d'uso:

---

---

---

---

\_\_\_\_\_   
Data richiesta

\_\_\_\_\_   
Timbro e Firma del Responsabile

\_\_\_\_\_   
Data Visto

\_\_\_\_\_   
Timbro e Firma del responsabile budget di Struttura

**Note:**

---

---

---

---

---

---

---

\_\_\_\_\_   
Firma referente sopralluogo

\* Compilazione riservata al personale del Servizio Informatico

---

---

---

---

---

---

---



## MODULO DI RICHIESTA PER ACQUISTO/AGGIORNAMENTO/SVILUPPO SOFTWARE

<b>RICHIEDENTE::</b> U.O.A./Ag. - Servizio - Ufficio _____				
Centro di Costo _____				
<b>Sede amministrativa</b>	<b>Ospedale</b>	<b>Distretto</b>	<b>Dip. di Prevenzione</b>	
Arzignano	Montecchio M.	Chiampo	Lonigo	Via Caboto (Arz.)
Valdagno	Castelgomberto	Cornedo	Recoaro	Altro _____

<b>Si richiede con la presente:</b>		
<b>NUOVA ACQUISIZIONE</b>	<b>AGGIORNAMENTO</b>	<b>SVILUPPO DAL S.I.L.</b>
Descrizione SOFTWARE (Marca/Nome/Versione o funzioni che deve svolgere) _____		
Da installare/aggiornare su N° _____ Personal Computers	Con pubblicazione su Server (Citrix/web, etc.)	
Presso la sede indicata	Presso altra/e sede/i: _____	

Previsione di costo complessivo del programma/aggiornamento (Euro) _____
Risorse aggiuntive necessarie:
MATERIALE DI CONSUMO (descrizione e spesa stimata) _____
PERSONALE (compresi costi per formazione) _____
ALTRO (compresi costi) _____
Ditte fornitrici _____

Motivazioni all'acquisto e risultati attesi dal punto di vista operativo _____

Altre annotazioni \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Data \_\_\_\_ / \_\_\_\_ / \_\_\_\_ Firma del richiedente \_\_\_\_\_

Data \_\_\_\_ / \_\_\_\_ / \_\_\_\_ Visto Responsabile budget di struttura \_\_\_\_\_



**Allegato G)** Modulo richiesta recupero dati



Alla c.a. Responsabile  
**Servizio Backup Dati**  
 U.O.C. Servizio Informatico  
 Via Trento 4 – 36071 Arzignano

Servizio/Reparto: .....

Responsabile: .....

Sede: .....

Tel.: .....

**Oggetto: Recupero dati da Backup**

Con la presente si chiede il recupero dei seguenti files/Cartelle :

File o cartella?	Percorso e nome file	Data presunta della perdita del dato	Data preferita per il ripristino
F C			
F C			
F C			
F C			
F C			
F C			

**Esempi**

<del>F C</del>	P:\sildoc\SICUREZZA\OpenVPN	12/10/2006	12/10/2006 o il più recente possibile.
<del>F C</del>	P:\sildoc\SICUREZZA\OpenVPN\Elenco_client_OpenVPN.xls	01/09/2006	Metà agosto

IL RESPONSABILE

.....



## Modulo Consegna materiale Informatico

Rev 1.0.4

<b>Inventario</b>		<b>Data Consegna</b>
<input type="text"/>		<input type="text"/>
<b>Marca</b>	<b>Tipo</b>	<b>Numero di Serie</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<b>Modello</b>	<b>Nome PC</b>	<b>Sostituisce Apparecchio</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<b>Utente- Riferimento</b>	<b>IP</b>	<b>MAC ADDRESS</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<b>Ubicazione (Ospedale-reparto-distretto ecc)</b>		
<input type="text"/>		
<b>N.Richiesta</b>	<b>Telefono</b>	<b>Tecnico Incaricato</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>

**Norme per la custodia Apparecchiature non istallate o portatili/mobili:**

Il dipendente assegnatario di una apparecchiatura elettronica portatile dell'ULSS è tenuto a custodirla con diligenza.

In particolare deve assicurarsi che:

1) L'apparecchiatura portatile/mobile sia sotto il suo diretto controllo o di propri collaboratori individuati

Non sia lasciata incostudita, salvo che in un locale di un fabbricato chiuso con chiave o con altri mezzi idonei di chiusura

2) Non sia lasciata incostudita su di un mezzo di trasporto, salvo che in un bagagliaio metallico di autoveicolo chiuso a chiave, dotato di antifurto funzionante ed unicamente nelle ore diurne (dalle 6 alle 20)

3) Il rispetto delle sopraindicate regole è condizione essenziale per il mancato addebito al dipendente del danno dell'Amministrazione conseguente all'eventuale furto/sottrazione dell'apparecchiatura portatile/mobile affidata al dipendente medesimo.

<b>Timbro e Firma del ricevente</b>	<b>Firma Leggibile (di chi consegna)</b>
_____	_____

Usato: No

**Allegato I) Modulo scheda registrazione attività di assistenza e riparazione**



Garanzia

<b>Ticket:</b>	<b>Data:</b>
<b>Ora Inizio:</b>	<b>Ora Fine:</b>
<b>Durata:</b>	

<input type="checkbox"/> Standard	<input type="checkbox"/> Reperibilità	<input type="checkbox"/> Installazione	<input type="checkbox"/> Non di competenza	<input type="checkbox"/> Spostamento definitivo
-----------------------------------	---------------------------------------	--	--	---

--	--

<input type="checkbox"/> PC-Terminale-Notebook	<input type="checkbox"/> Monitor	<input type="checkbox"/> Stampante	<input type="checkbox"/> Scanner	<input type="checkbox"/> Server	<input type="checkbox"/> Lettore BC
--	----------------------------------	------------------------------------	----------------------------------	---------------------------------	-------------------------------------

<input type="checkbox"/> Sostituzione	<input type="checkbox"/> Ritiro	<input type="checkbox"/> Trasferimento-Manutenzione	<input type="checkbox"/> Rete	<input type="checkbox"/>
---------------------------------------	---------------------------------	---	-------------------------------	--------------------------

--	--

--	--

Monitor	Stampante	Scanner	Altro	PC
---------	-----------	---------	-------	----

--	--	--	--

	<input type="checkbox"/> Intervento sospeso
--	---

--	--

--	--

--	--	--