REGOLAMENTO PER L'UTILIZZO DEL SISTEMA INFORMATICO AZIENDALE

Approvato il	Nome	Funzione
02/12/2015	Ing. Andrea Oliani	Direttore UOC Sistema Informativo ed Informatico

INDICE

1. **SCOPO**

Il presente regolamento ha lo scopo di disciplinare le modalità di accesso e di uso del Sistema Informatico dell'ULSS 20 di Verona e dei servizi che, tramite di esso, è possibile ricevere o offrire all'interno e all'esterno dell'Azienda.

1.1 **Strumenti Informatici e Patrimonio Informativo**

In particolare si specifica che il Sistema Informatico dell'ULSS 20 di Verona è costituito dall'insieme degli Strumenti Informatici, cioè dalle risorse infrastrutturali che lo compongono, e dal Patrimonio Informativo in formato elettronico che, attraverso di essi, viene prodotto, aggiornato e consultato.

- Gli Strumenti Informatici sono costituiti da tutte le componenti hardware e software in uso e da quelle della rete di trasmissione dati (con riferimento al "dominio aziendale", ovvero alla rete di computer gestita attraverso il sistema di controllo centrale dell'ULSS20).
- Il Patrimonio Informativo è l'insieme delle banche dati in formato digitale ed in generale di tutti i documenti in formato elettronico prodotti e resi disponibili tramite l'utilizzo dei suddetti strumenti.

2. **CAMPO DI APPLICAZIONE**

Il presente regolamento si applica a tutti gli Utenti Interni ed Esterni che sono autorizzati ad accedere al Sistema Informatico Aziendale.

2.1 **Utenti interni e esterni**

Per Utenti Interni si intendono le persone fisiche che, sulla base di rapporti contrattuali o convenzionali autorizzati dalla Direzione dell'Azienda, possono utilizzare all'interno del "dominio aziendale" gli strumenti informatici dell'ULSS20 di Verona.

Per Utenti Esterni si intendono: le persone fisiche, le Aziende private e Pubbliche e le ditte fornitrici che, sulla base di rapporti contrattuali o convenzionali autorizzati dalla Direzione dell'Azienda, accedono dall'esterno del "dominio aziendale" ad alcune componenti del Sistema Informatico Aziendale.

3. **RESPONSABILITA'**

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle Risorse Informatiche, dell'utilizzo dei servizi/programmi ai quali ha accesso e delle informazioni che tratta. L'assegnazione di risorse informatiche aziendali non ne comporta il possesso, in quanto trattasi di strumenti di esclusiva proprietà aziendale. Gli utenti interni utilizzano, nel proprio lavoro, soltanto strumenti informatici assegnatigli dall'Azienda ULSS 20. L'uso di computer privati deve essere preventivamente autorizzato dal Direttore dell'UOC Sistema Informativo ed Informatico. Per motivi di sicurezza e protezione dei dati, oltre che per ottemperare alle normative vigenti (tra cui il D.Lgs. 196/03 detto "della Privacy"), ogni attività svolta con il

Sistema Informatico Aziendale è sottoposta a registrazione in appositi file (log) con riferimento alle credenziali dell'utente e alla stazione di lavoro utilizzata. Detti file possono essere utilizzati per attività di monitoraggio e controllo del buon funzionamento del Sistema Informatico Aziendale da parte degli Amministratori di Sistema, e possono essere messi a disposizione della Direzione Aziendale e dell'Autorità Giudiziaria nei casi previsti dalla normativa. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. 196/03. Ciascun Dirigente di U.O. ha la responsabilità di vigilare e verificare il corretto utilizzo degli strumenti informatici assegnati alla propria U.O. e di evitare l'uso improprio o l'accesso da parte di personale non autorizzato, richiedendo all'U.O.C. Sistema Informativo ed Informatico gli eventuali interventi necessari.

4. **MODALITA' OPERATIVE**

4.1 **Utilizzo delle stazioni di lavoro**

- I personal computer ed i dispositivi mobile aziendali utilizzati dagli Utenti Interni sono strumenti di lavoro. Ogni utilizzo improprio può causare disservizi, costi impropri di manutenzione e, soprattutto, minacce alla sicurezza ed alla privacy.
- L'accesso alle stazioni di lavoro avviene tramite credenziali individuali che devono essere custodite dall'utente con la massima diligenza e non divulgate a terzi per alcun motivo. Vengono utilizzate credenziali di accesso anche per tutti i servizi/programmi disponibili e per lo screen saver.
- Non è consentita l'attivazione della password di accensione (bios).
- Non è consentito installare autonomamente programmi di alcun tipo sulle stazioni di lavoro. In caso di necessità di acquisto o dotazione di software applicativi e/o app (che devono comunque risultare pertinenti esclusivamente alle attività istituzionali da svolgersi), deve essere preventivamente formulata richiesta scritta (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico, che valuterà la compatibilità funzionale, tecnica e di budget della richiesta. L'installazione non autorizzata di software induce grave rischio di infezioni da virus informatici o di malfunzionamenti degli strumenti informatici aziendali.
- Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'ULSS 20 di Verona (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore).
- Non è consentito all'utente di modificare le caratteristiche impostate sulle stazioni di lavoro che utilizza, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi aziendali.
- La stazione di lavoro non deve essere lasciata accesa e incustodita, al fine di evitarne l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Compatibilmente con le esigenze operative di servizio, gli utenti interni devono "bloccare" la

postazione prima di assentarsi temporaneamente (combinazione di tasti WINDOWS+L) e spegnerla al termine dell'attività lavorativa. La necessità di modalità operative diverse da quelle indicate deve essere segnalata per iscritto (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico, al fine di valutare eventuali soluzioni "specifiche".

- Non è consentita l'installazione sulle stazioni di lavoro aziendali, o il collegamento sulla rete, di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili ed apparati in genere …), se non con l'autorizzazione espressa del Direttore dell'UOC Sistema Informativo ed Informatico, previa richiesta scritta da parte del Direttore dell'UOC.
- Ogni utente deve prestare la massima attenzione nell'uso di supporti quali penne USB, avvertendo immediatamente l'UOC Sistema Informativo ed Informatico nel caso in cui siano rilevati virus, ed adottando quanto previsto dal successivo punto 13 del presente Regolamento in relazione alle procedure di protezione antivirus.
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

4.2 **Utilizzo di cartelle condivise**

- Le cartelle condivise sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia strettamente pertinente all'attività lavorativa non può essere memorizzato in queste unità. Sulle cartelle condivise sono svolte regolari attività di monitoraggio e amministrazione da parte del personale dell'UOC Sistema Informativo ed Informatico.
- La creazione di cartelle condivise deve essere richiesta per iscritto (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico, motivandone la necessità e l'elenco degli utenti che devono essere autorizzati all'accesso.
- Anche l'accesso alle cartelle condivise avviene tramite credenziali individuali.
- Il personale dell'UOC Sistema Informativo ed Informatico può in qualunque momento procedere alla rimozione di ogni file o applicazione che risulti pericolosa per la sicurezza del Sistema Informatico Aziendale.
- La rimozione di file non pertinenti all'attività istituzionale, sia dalle stazioni di lavoro sia dalle cartelle condivise, verrà concordata dall'UOC Sistema Informativo ed Informatico con il Direttore dell'UOC di competenza.
- Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti da evitarsi un'archiviazione ridondante.

4.3 **Modalità di accesso alla rete e ai servizi/programmi per gli utenti interni**

- A tutti i dipendenti dell'ULSS20 di Verona è assegnata una casella di mail aziendale, accessibile tramite credenziali individuali.
- Per essere autorizzati all'uso di qualunque altra risorsa informatica è necessario che venga presentata al Direttore dell'UOC Sistema Informativo ed Informatico, da parte del Direttore della propria UOC, una richiesta scritta (via mail).
- L'UOC Sistema Informativo ed Informatico provvede ad assegnare ad ogni utente le credenziali per ogni servizio/programma autorizzato. Le credenziali sono costituite dall'accoppiamento di un codice personale o Username con una Password. Per ogni servizio/programma vengono abilitate all'utente solo le funzioni per le quali è stato autorizzato (profilazione).
- Non sono previste credenziali "anonimi", ovvero non riconducibili al singolo utente.
- Nei casi (eccezionali) di creazione di credenziali "generiche" (per es. denominazione dell'UO) la responsabilità del relativo utilizzo è attribuita al Direttore dell'UOC di competenza.

4.4 **Modalità di accesso alla rete e ai servizi/programmi per gli utenti esterni**

- L'accesso al Sistema Informatico Aziendale da parte degli utenti esterni può avvenire sostanzialmente con due differenti modalità:
  1. accesso con credenziali individuali (per singolo operatore, nel caso di Ente o Azienda) ai servizi/programmi dell'ULSS20, esattamente come per gli utenti interni
  2. accesso attraverso soluzioni di "cooperazione applicativa".
- In ogni caso è necessario che gli utenti esterni interessati presentino richiesta scritta e motivata al Direttore dell'UOC Sistema Informativo ed Informatico, specificando le funzionalità richieste e l'elenco nominativo delle persone da abilitarsi ed i relativi "profili" di abilitazione.
- L'UOC Sistema Informativo ed Informatico attiva, per gli utenti esterni, specifiche modalità per la realizzazione di un collegamento informatico sicuro e criptato (VPN).
- Fanno eccezione a tali regole le iniziative imposte da normative nazionali o regionali che prevedano specifiche modalità tecnologiche di interazione informatica (es. prescrizione dematerializzata di MMG/PLS).

4.5 **Gestione delle password**

- Le credenziali utilizzate, Username e Password, sono strettamente personali; la loro tutela è a carico dell'utente. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico.

- Ai fini dell'assistenza all'utente, la password di accesso può essere comunicata agli operatori tecnici chiamati ad intervenire, i quali ne assicurano la riservatezza e la tutela, invitando l'utente a provvedere immediatamente, dopo l'intervento, alla sua sostituzione.
- La password deve essere lunga almeno 8 caratteri, non deve avere riferimenti diretti con dati personali dell'utente (data di nascita, nome, cognome, nome dei figli, ecc.) o ad esso facilmente riconducibili, deve essere alfanumerica e rispettare almeno 3 dei seguenti 4 requisiti: almeno una lettera maiuscola, almeno una lettera minuscola, almeno un numero, almeno un carattere speciale.
- Le password utilizzate hanno una durata massima, generalmente di tre mesi, trascorsi i quali le password devono essere sostituite da parte degli utenti.
- La password deve essere immediatamente sostituita nel caso si sospetti che la stessa sia a conoscenza di terzi.
- Qualora l'utente venisse a conoscenza della password di un altro utente, è tenuto a darne immediata notizia all'interessato al fine che quest'ultimo provveda alla sostituzione.
- E' dato incarico ai Direttori di UOC di comunicare tempestivamente per iscritto (via mail) al Direttore dell'UOC Sistema Informativo ed Informatico eventuali cambi di mansioni dei propri collaboratori che comportino modifiche o revoche di autorizzazione all'accesso alle risorse informatiche, al fine di rendere possibili le modifiche dei profili di accesso alle risorse stesse e la sostituzione delle password ove necessario.

4.6 **Utilizzo di supporti di memorizzazione**

- Tutti i supporti di memorizzazione (dischetti, cassette, cartucce, cd-rom, dvd, chiavette USB, ecc.) contenenti dati o documenti aziendali, in particolar modo se sensibili, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
- I supporti di memorizzazione contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
- I supporti di memorizzazione non più fruibili per qualsiasi motivo devono essere distrutti fisicamente.
- Non è consentito importare sulla stazione di lavoro aziendale, o su risorse dell'Azienda, file non aventi alcuna attinenza con la propria attività lavorativa.
- Tutti i file di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo da parte del personale dell'UOC Sistema Informativo ed Informatico.

4.7 **Utilizzo di PC portatili**

- I PC portatili vengono assegnati individualmente a singoli utenti interni, che rispondono del loro utilizzo e devono custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo intra ed extra aziendale.
- Se l'utilizzo del PC portatile è condiviso da più utenti il PC è assegnato al Direttore dell'UOC di competenza.
- Ai PC portatili si applicano le medesime regole di utilizzo previste per le stazioni di lavoro connesse in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

4.8 **Utilizzo delle stampanti e dei materiali di consumo**

- L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come cd-rom e dvd) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi non motivati.
- E' tassativamente vietato lasciare incustoditi presso le stampanti documenti cartacei contenenti dati personali/sensibili o comunque riservati.
- E' compito dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può e deve essere cancellata.

4.9 **Utilizzo della posta elettronica aziendale**

- A tutti i dipendenti dell'ULSS20 di Verona è assegnata una casella di mail aziendale, accessibile tramite credenziali individuali.
- E' vietato l'utilizzo, dalle stazioni di lavoro aziendali, di altri sistemi di posta elettronica; in generale, infatti, i sistemi di mail non aziendali non garantiscono adeguate misure di sicurezza e protezione, esponendo quindi sia l'utilizzatore sia l'ULSS20 a rischi di "infezioni informatiche" del proprio sistema.
- Il dipendente risponde in proprio degli eventuali danni/costi causati all'ULSS20 a causa dell'utilizzo di sistemi di posta elettronica diversi da quello aziendale.
- Vengono attivati indirizzi di posta elettronica per le strutture aziendali, che possono essere condivisi da più operatori, secondo le necessità che devono essere dichiarate per iscritto (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico.
- Possono inoltre essere attivati indirizzi di posta elettronica individuali per le altre tipologie di utenti interni, sempre secondo le necessità che devono essere dichiarate per iscritto (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico.

- In ogni caso la casella di mail non è uno strumento di lavoro "riservato", in quanto strumento di esclusiva proprietà aziendale messo a disposizione dell'utente al solo fine dello svolgimento delle proprie attività lavorative.
- La casella di posta elettronica, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Si rammenta che i normali sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, gli utenti non devono inoltrare dati ed informazioni classificabili come "sensibili" o "riservate" con questo mezzo.
- La normativa sulla Privacy vieta l'utilizzo delle caselle di mail per la trasmissione di informazioni personali e/o sensibili.
- E' tassativamente vietato l'uso della Posta Elettronica per la trasmissione di materiale pedofilo/pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno. Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.
- Non si devono utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list non attinenti la propria attività istituzionale. Viene ammesso invece l'utilizzo, al di fuori dell'orario di servizio, della mail aziendale per attività inerenti le relazioni sindacali e le attività legate ai circoli aziendali che rimangano nell'ambito dell'ULSS 20.
- La casella di posta elettronica deve essere mantenuta in ordine, cancellando regolarmente documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei sistemi stessi.
- Ogni comunicazione inviata o ricevuta da corrispondenti esterni all'Azienda che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'ULSS 20 di Verona, ovvero contenga documenti da considerarsi riservati, deve essere visionata ed autorizzata dal Dirigente di competenza dell'attività in questione e trasmessa esclusivamente attraverso caselle di posta certificata (PEC).
- Per la trasmissione di file all'interno dell'Azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
- E' vietato aprire od eseguire file allegati alla posta elettronica se non si è certi del mittente e del loro contenuto.
- E' vietato partecipare alle cosiddette catene telematiche (o di "Sant'Antonio"), e non si devono in alcun caso attivare gli allegati di tali messaggi.
- E' severamente vietato eseguire o favorire pratiche di spamming.
- Ciascun utente può, anche da postazioni esterne all'azienda, utilizzare la propria casella di posta elettronica aziendale.

- In caso di assenza è opportuno attivare messaggi di risposta automatica che informino il mittente della propria indisponibilità, ed eventualmente anche l'inoltro automatico dei messaggi ricevuti verso indirizzi di altri utenti..
- Nel caso in cui un utente interno si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, un fiduciario, da lui preventivamente nominato, o, in sua assenza, il Direttore della UOC , potrà accedere alla casella di posta al fine di garantire la continuità dell'attività lavorativa. La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e consegnata al responsabile dell'U.O.

4.10 **Utilizzo della rete internet e dei relativi servizi**

- La stazione di lavoro abilitata alla navigazione in Internet costituisce sempre e comunque uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
- E' consentito l'uso dell'accesso ad internet anche per motivi personali purché tale utilizzo sia occasionale, limitato nel tempo, confinato all'esterno dell'orario di lavoro, non pregiudizievole dell'uso dei sistemi da parte degli altri utenti né della efficienza ed efficacia della prestazione lavorativa, né della sicurezza del sistema informativo aziendale, e comunque per finalità lecite.
- Data la vastissima gamma di attività istituzionali svolte in Azienda, risulta di fatto impossibile stabilire a priori un elenco di siti autorizzati; per garantire il corretto utilizzo della navigazione in Internet vengono comunque utilizzati appositi strumenti di filtraggio, gestiti a livello aziendale, mediante i quali viene bloccata la navigazione su categorie e/o singoli siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività aziendali. Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.
- L'accesso a specifici siti che risultino "oscurati" sulla base della policy aziendale può essere richiesto, illustrandone le motivazioni, per iscritto (via mail) dal Direttore dell'UOC di riferimento al Direttore dell'UOC Sistema Informativo ed Informatico.
- Non è consentito all'utente lo scarico di software gratuito (freeware) e shareware da siti Internet.
- Agli utenti interni è vietata la registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- Non è permessa, tramite la rete aziendale, la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.
- Il Direttore dell'UOC Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
- E' tassativamente vietato visitare siti e/o memorizzare documenti informatici dai contenuti di natura pedofilo/pornografica, fraudolenta/illegale, riguardante il gioco d'azzardo, blasfema e/o

molesta/oscena, oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

- Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti visitati dalle stazioni di lavoro aziendali. L'accesso a questi dati è effettuato dal personale della UOC Sistema Informativo ed Informatico ed eventualmente da personale tecnico esterno autorizzato dalla direzione della UOC Sistema Informativo ed Informatico.
- I sistemi aziendali sono programmati e configurati in modo da cancellare semestralmente i dati relativi agli accessi ad Internet ed al traffico telematico. L'eventuale prolungamento dei suddetti tempi di conservazione é eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

4.11 **Protezione antivirus**

- Tutte le stazioni di lavoro collegate alla rete aziendale sono dotate di uno specifico sw antivirus.
- Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
- Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
  - sospendere ogni elaborazione in corso senza spegnere il computer;
  - segnalare l'accaduto al personale dell'UOC Sistema Informativo ed Informatico.
- Non è consentito l'utilizzo di cd rom, cd riscrivibili, dvd, nastri magnetici e ogni altro supporto di memorizzazione di provenienza ignota.
- Ogni dispositivo di memorizzazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al personale dell'UOC Sistema Informativo ed Informatico per la verifica della possibilità di "bonifica" del supporto.

4.12 **Teleassistenza**

- Per le attività di manutenzione remota sulle stazioni di lavoro connesse alla rete aziendale, il personale tecnico dell'UOC Sistema Informativo ed Informatico ed i tecnici esterni che vi operano utilizzano specifici software.
- Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene previo avviso all'utente interessato che può rifiutare tale tipo di assistenza allungando però in questa maniera i tempi d'intervento. L'attivazione del software di intervento da remoto prevede un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso alla stazione di lavoro.

4.13 **Controlli**

- Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:
    - analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (sede, reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni)
    - emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
    - in caso di successivo permanere di una situazione non conforme, é possibile effettuare controlli circoscritti su singole postazioni di lavoro.
- Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:
    - analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
    - emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
    - in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

4.14 **Non osservanza delle regole aziendali**

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere al Sistema Informatico Aziendale ed ai servizi/programmi precedentemente autorizzati, fatte salve le sanzioni disciplinari, previste dalla normativa vigente in materia e dai regolamenti interni, che possono essere comminate e ulteriori conseguenze di natura penale, civile e amministrativa.

4.15 **Informativa ai sensi dell'art. 13 del D.Lgs. 196/03**

Il Titolare del trattamento dei dati personali della presente direttiva è l'Azienda ULSS 20 di Verona.

I diritti previsti dall'art. 7 D.Lgs. 196/03, ed in particolare il diritto di conoscere i dati che riguardano l'utente, il diritto di aggiornarli e il diritto di cancellare i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi per iscritto (via mail) all'UOC Sistema Informativo ed Informatico.