



Servizio Sanitario Nazionale – Regione dell'Umbria
AZIENDA UNITA' SANITARIA LOCALE UMBRIA 1
Sede Legale Provvisoria: Via Guerra 21 – Perugia
Codice Fiscale e Partita IVA 03301860544

DELIBERA DEL DIRETTORE GENERALE
n. 1524 del 28/11/2018

Proponente: UO Tecnologie Informatiche e Telematiche

Oggetto: Approvazione del Disciplinare per il corretto utilizzo degli strumenti informatici e telematici, internet e posta elettronica.

IL DIRETTORE GENERALE

Vista la proposta di delibera in oggetto di cui al num. Provv 16716 del 26/11/2018 contenente:

il Parere del Direttore Amministrativo – Dott.ssa Doriana SARNARI

il Parere del Direttore Sanitario – Dr. Pasquale PARISE

Hash .pdf (SHA256):

bd3491c8f381da2db0bbbe0e321bcb6a370f5cdbd7003ecdbc9f41139eb4be69

Hash .p7m (SHA256):

3c815f47cb95ebafae8472f94b2edb42cbde73357eb79bc2bd8f984f488d0062

Firme digitali apposte sulla proposta:

Pasquale Parise, Fabrizio Papalini, Barbara Gamboni, Doriana Sarnari, Domenico Barzotti

DELIBERA

Di recepire la menzionata proposta di delibera che allegata al presente atto ne costituisce parte integrante e sostanziale e di disporre quindi così come in essa indicato.

IL DIRETTORE GENERALE
(Dott. Andrea CASCIARI)*

DOCUMENTO ISTRUTTORIO

Oggetto: Approvazione del Disciplinare per il corretto utilizzo degli strumenti informatici e telematici, internet e posta elettronica.

PREMESSO

CHE con l'entrata in vigore della direttiva del Presidente del Consiglio dei Ministri 1 Agosto 2015 e relativa circolare AGiD del 17 Marzo 2017, avente ad oggetto "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" e successivamente con l'entrata a regime del Regolamento Generale sulla Protezione dei Dati (GDPR), questa Azienda Usl ha avviato un percorso di aggiornamento e rafforzamento delle proprie politiche di sicurezza informatica;

CHE in tale percorso assume particolare rilevanza la definizione delle istruzioni per gli utenti interni, al fine di minimizzare i comportamenti non corretti ed aumentare la consapevolezza sui rischi connessi all'utilizzo della tecnologia;

VALUTATA la crescente pervasività delle tecnologie dell'informazione e di comunicazione e la rapida evoluzione tecnologica, e ritenuto necessario procedere all'aggiornamento del vigente disciplinare per il Corretto Utilizzo degli Strumenti Informatici e Telematici, Internet e Posta elettronica di cui alla nota del Direttore Generale n. 525927/2013;

DATO ATTO che le regole definite nel nuovo disciplinare sono da ritenersi vincolanti per tutti i soggetti che utilizzano gli strumenti informatici o che accedono alla rete informatica dell'Azienda USL Umbria 1 (dipendenti, collaboratori, fornitori ecc.), al fine di contenere i rischi di perdita di dati e blocco della continuità operativa;

CHE in data 04/10/2018 il disciplinare in oggetto è stato trasmesso alle OO.SS. e alla RSU aziendale e che non sono pervenute osservazioni;

RITENUTO doveroso vigilare affinché tutti i dipendenti, i nuovi assunti e tutti i collaboratori che utilizzano a vario titolo i sistemi informatici aziendali, siano messi a conoscenza delle regole contenute nel disciplinare in oggetto;

si propone di adottare il seguente dispositivo:

1. **Approvare** il *Disciplinare per il corretto utilizzo degli strumenti informatici e telematici, internet e posta elettronica*, allegato al presente atto del quale costituisce parte integrante e sostanziale;
2. **Stabilire** che il Disciplinare di cui al punto 1 entra in vigore alla data di approvazione del presente atto ed è vincolante per tutti i soggetti che utilizzano gli strumenti informatici o che accedono alla rete informatica dell'Azienda USL Umbria1;
3. **Dare mandato** al Dirigente del Servizio Tecnologie Informatiche e Telematiche di:
 - a. Adottare le eventuali procedure operative necessarie per l'applicazione del Disciplinare di cui al punto 1 e per il suo adeguamento agli aggiornamenti tecnologici;

- b. Pubblicare sulla intranet aziendale il Disciplinare e le relative procedure operative e trasmettere il documento a tutte le articolazioni aziendali perché ne sia data comunicazione a tutti i dipendenti e a tutti i soggetti interessati;
4. **Disporre** che la U.O. Trattamento giuridico del personale dipendente consegna, all'atto della stipula del contratto di assunzione o di rapporto libero professionale, copia del disciplinare in oggetto;
 5. **Disporre** che la U.O. e Trattamento economico personale dipendente e gestione personale convenzionato comunichi, all'atto della nomina del personale convenzionato, l'obbligo di attenersi al regolamento in oggetto;
 6. **Dare mandato ai Designati al trattamento dati**, così come individuati nella Delibera n.1446 del 7/11/2018 ovvero: i Dirigenti delle Unità Operative, i Servizi di Staff e tutti gli operatori con incarico funzionale, di comunicare a tutte le risorse umane assegnate l'avvenuta approvazione del nuovo *Disciplinare per il Corretto Utilizzo degli Strumenti Informatici e Telematici, Internet e Posta elettronica* e di controllare che sia rispettato con diligenza;
 7. **Dare atto** che il presente provvedimento è soggetto a pubblicazione integrale ai sensi delle vigenti normative in tema di riservatezza;

**IL RESPONSABILE P.O.
TECNOLOGIE INFORMATICHE E
SISTEMI DI RETE**
Dott. Fabrizio Papalini

**IL DIRIGENTE U.O. TECNOLOGIE
INFORMATICHE E TELEMATICHE**
Dott. Ing. Barbara Gamboni

**DIRIGENTE U.O. RISORSE UMANE
TRATTAMENTO GIURIDICO
PERSONALE DIPENDENTE**
Dott. Domenico Barzotti

**Disciplinare per il Corretto
Utilizzo degli Strumenti
Informatici e Telematici, Internet
e Posta elettronica**

Sommario

SOMMARIO	2
1.1. Termini e abbreviazioni	5
1.2. Scopo e campi di applicazione	6
1.3. Esclusione all'uso degli strumenti informatici	8
1.4. Titolarità dei dispositivi e dei dati	8
1.5. Finalità nell'utilizzo dei dispositivi	9
1.6. Restituzione dei dispositivi	9
1.7. Assistenza tecnica informatica	9
2. SEZIONE II - CREDENZIALI	9
2.1. Le credenziali di autenticazione	10
2.2. Le password	10
2.3. Regole per la corretta gestione delle password	11
3. SEZIONE III - OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO	12
3.1. Login e Logout	12
3.2. Obblighi	12
4. SEZIONE IV - USO DEI DISPOSITIVI DELL'AZIENDA	13
4.1. Modalità d'uso del computer aziendale	13
4.2. Corretto utilizzo del computer aziendale	13
4.3. Divieti espressi sull'utilizzo dei computer	14
4.4. Antivirus	15

5. SEZIONE V – RETE LOCALE AZIENDALE	15
6. SEZIONE VI – INTERNET	16
6.1. Internet è uno strumento di lavoro	16
6.2. Misure preventive per ridurre navigazioni illecite	16
6.3. Divieti espressi concernenti Internet	16
6.4. Divieti di manomissione dei sistemi di sicurezza	17
6.5. Diritto d'autore	17
7. SEZIONE VII – POSTA ELETTRONICA	17
7.1. La Posta Elettronica	17
7.2. Divieti espressi	18
7.3. Posta Elettronica in caso di assenze o cessazione	19
8. SEZIONE VIII – USO DI ALTRI DISPOSITIVI (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE ED ALTRI DISPOSITIVI ELETTRONICI)	19
8.1. L'utilizzo del notebook, tablet o smartphone.	19
8.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)	20
8.3. Dispositivi personali	21
8.4. Distruzione dei Dispositivi	21
9. SEZIONE IX – SISTEMI IN CLOUD	21
10. SEZIONE X – ACCESSO AUTORIZZATO DALL'ESTERNO MEDIANTE VPN	21
11. SEZIONE XI – APPLICAZIONE E CONTROLLO	22
11.1. Il controllo	22

11.2. Modalità di verifica	22
11.3. Modalità di conservazione	23
12. SEZIONE XII – VALIDITÀ E PUBBLICAZIONE	24
12.1. Validità	24
12.2. Pubblicazione	24

GRUPPO DI LAVORO

Nominativo	Funzione
Barbara Gamboni	<i>Responsabile U.O. Tecnologie Informatiche e Telematiche</i>
Fabrizio Papalini	<i>P.O. Tecnologie Informatiche e Sistemi di Rete</i>
Fabio Frinai	<i>Programmatore U.O. Tecnologie Informatiche e Telematiche</i>
Luca Bondi	<i>Collaboratore Professionale Programmatore U.O. Tecnologie Informatiche e Telematiche</i>

1.1. Termini e abbreviazioni

Azienda: l'Azienda Usl Umbria 1

Antivirus: programma che individua, previene e disattiva o rimuove programmi dannosi, come virus e worms.

Autorizzato al trattamento dei dati personali: ogni incaricato, come di seguito identificato che, nell'ambito dell'attività assegnatagli, tratta dati personali.

Backup: copia di riserva di un disco, di una parte del disco o di uno o più file su supporti di memorizzazione diversi da quello in uso.

Chat: servizio che permette mediante apposito software una 'conversazione' fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.

Chiave USB: o unità flash USB o penna USB (anche in inglese USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

Client: computer o programma collegato a un altro (computer o programma) a cui inoltra le richieste dell'incaricato.

Cloud computing: in informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Dati: l'insieme di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Azienda) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR).

Dispositivi (dispositivo): personal computer e altra unità hardware quale periferica/dispositivo elettronico, anche ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet PC ecc.).

Dipendente: personale che presta servizio presso l'Azienda il cui rapporto può essere regolato con diverse forme contrattuali, comprende anche personale in stage o tirocinio.

File: porzione di memoria (fissa o mobile) che contiene un insieme organizzato di informazioni omogenee.

File sharing: condivisione di file all'interno di una rete di calcolatori e tipicamente utilizza una delle seguenti architetture: client-server, peer-to-peer (rete informatica in cui i nodi sono gerarchizzati sotto forma di nodi equivalenti o paritari (in inglese peer) che possono cioè fungere sia da client che da server verso gli altri nodi della rete).

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Incaricato: ogni soggetto al quale è concesso l'utilizzo di strumenti informatici o che accede alla rete informatica dell'Azienda. Ricomprende anche la categoria degli "Autorizzati al trattamento di dati personali", quando il trattamento dei dati è effettuato con strumenti informatici.

LOG: file costituito da un elenco cronologico delle attività svolte da un sistema operativo, da un database o da altri programmi, generato per permettere una successiva verifica.

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, sottrarre informazioni o dati, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

Postazione di lavoro: postazione attrezzata e dotazione tecnica necessaria per svolgere un'attività lavorativa, comprende ad esempio personal computer ed eventuali altre unità hardware.

Phishing: tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione mail.

Repository: In un repository sono raccolti dati e informazioni in formato digitale, valorizzati e archiviati sulla base di metadati che ne permettono la rapida individuazione, anche grazie alla creazione di tabelle relazionali. Grazie alla sua peculiare architettura, un repository consente di gestire in modo ottimale anche grandi volumi di dati.

Rete locale: una Local Area Network (sigla inglese: LAN - in italiano: rete locale) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

Server: computer o programma a cui altri (computer o programmi) si collegano per l'elaborazione delle richieste dell'incaricato.

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

VPN: una Virtual Private Network, cioè una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet.

1.2. Scopo e campi di applicazione

Scopo del disciplinare è tutelare il patrimonio dell'Azienda, garantire il corretto trattamento dei dati personali così come previsto dalla normativa vigente ed assicurare la massima continuità operativa dei sistemi informatici.

Con l'entrata in vigore delle Misure Minime per la Sicurezza Informatica della Pubblica Amministrazione (CIRCOLARE AGID 18 aprile 2017, n. 2/2017) e la definitiva applicazione del Regolamento Europeo per la Protezione dei Dati Personali (GDPR), l'Azienda ha la necessità di

innalzare e rafforzare la tutela e la protezione dei dati personali dei propri dipendenti e dei cittadini che usufruiscono dei servizi sanitari.

Ai fini di questo disciplinare si specifica, comunque, che con il termine **“dati”** deve intendersi l’insieme più ampio di informazioni di cui un dipendente o un collaboratore (a prescindere dal tipo di rapporto contrattuale con l’Azienda) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i **“dati personali”** intesi a norma di legge.

In linea generale, ogni dato, nell’accezione più ampia sopra descritta, di cui l’incaricato viene a conoscenza, nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto di collaborazione con l’Azienda stessa o qualora le informazioni siano di pubblico dominio), salvo specifica autorizzazione esplicita dell’Azienda.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l’accesso alla rete internet dal computer aziendale espone l’Azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all’immagine dell’Azienda stessa.

Premesso che i comportamenti che normalmente si adottano nell’ambito di un rapporto di lavoro, tra i quali rientrano l’utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l’Azienda ha adottato il presente Disciplinare diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati, delle attrezzature e dei servizi aziendali.

Un uso dei dispositivi nonché dei servizi di accesso alle rete aziendale o alla rete internet (di seguito internet), alle applicazioni aziendali e/o della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l’Azienda ad un incremento della minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell’intero sistema informatico.

L’Azienda USL Umbria n.1 si ispira ai principi fissati dall’ articolo 5 del Regolamento UE 2016/679 (GDPR) ed opera in modo tale che ogni trattamento di dati personali avvenga nel rispetto dei seguenti principi:

- Liceità, correttezza e trasparenza del trattamento, nei confronti dell’interessato;
- Limitazione della finalità del trattamento, compreso l’obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- Minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- Esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- Limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- Integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento;

- Principio di necessità, secondo cui i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite e che i dati personali sono trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi;
- Principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime;
L'Azienda tratta i dati "nella misura meno invasiva possibile", cioè le attività di monitoraggio sono svolte solo dai soggetti preposti e sono mirate sulla sola area interessata, definita di rischio, tenendo conto della normativa sulla protezione dei dati e del principio di segretezza della corrispondenza;
- Principio di trasparenza che impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Il presente Disciplinare si applica agli incaricati che si trovino ad operare con dati o strumenti dell'Azienda. La mancata osservanza delle disposizioni contenute nel presente disciplinare può comportare gravi danni all'Azienda. Tale evento costituisce pertanto un grave inadempimento dei compiti assegnati e potrebbe avere gravi conseguenze sia sotto il profilo disciplinare che penale.

Le procedure operative, conformi al contenuto del presente Disciplinare e necessarie per la sua applicazione, saranno emesse dall'U.O. Tecnologie Informatiche e Telematiche e comunicate a tutti gli Incaricati.

1.3. Esclusione all'uso degli strumenti informatici

Nell'affidamento di mansioni o incarichi l'Azienda valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, dell'accesso ad internet, della posta elettronica e più in generale di tutti i servizi informatici e di telecomunicazioni da parte degli incaricati.

Al venir meno delle esigenze per detto utilizzo dei dispositivi aziendali, delle applicazioni aziendali, di internet e della posta elettronica, l'Azienda provvede a revocare l'autorizzazione.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità precedentemente citato. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

1.4. Titolarità dei dispositivi e dei dati

L'Azienda è esclusiva titolare dei dispositivi messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa. L'assegnazione, la gestione, la custodia e la dismissione di detti beni è disciplinata dai Regolamenti sulla gestione dei beni mobili ai quali integralmente si rimanda.

L'Azienda è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali.

Eventuali dati personali di natura privata dell'incaricato non devono essere salvati nei dispositivi messi a disposizione dall'Azienda.

I dispositivi assegnati agli incaricati possono essere, per esigenze organizzative, riassegnati ad altre persone all'interno dell'Azienda. In questi casi il dispositivo viene formattato e ripristinato alle configurazioni iniziali. Eventuali dati, anche di carattere personale (inclusi i messaggi di posta elettronica inviati o ricevuti, i file di immagini o video ed altre tipologie di file) se di interesse, devono essere rimossi dall'incaricato prima della restituzione del dispositivi. L'Azienda non assume responsabilità circa la perdita di dati personali dell'incaricato contenuti nei dispositivi aziendali.

1.5. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali. Eventuali deroghe all'utilizzo degli strumenti per fini personali devono essere autorizzate, su richiesta del Responsabile del Servizio in cui opera l'Incaricato, dalla Direzione Generale.

Qualsiasi eventuale tolleranza da parte di questa Azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'Azienda, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dispositivi in uso alla U.O. Tecnologie Informatiche e Telematiche;
2. Divieto assoluto di formattare, alterare, manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

Le stesse regole si applicano anche in caso di restituzione del dispositivo in seguito a richiesta di manutenzione per guasto del dispositivo o in caso di controlli che l'Azienda è tenuta ad effettuare sul dispositivo stesso.

1.7. Assistenza tecnica informatica

L'assistenza tecnica informatica deve essere attivata mediante l'apposito numero telefonico di help desk, attivo in orario diurno feriale, oppure mediante il software di richiesta di assistenza tecnica (trouble ticketing). Altre modalità di contatto con l'U.O. Tecnologie Informatiche e Telematiche per l'attivazione del servizio assistenza impediscono la corretta tracciatura della richiesta e non garantiscono l'esito e l'efficienza dell'intervento.

Per servizi o sistemi di particolare criticità sono attivati specifici servizi di assistenza tecnica informatica h24, le cui modalità di utilizzo sono regolate da procedure operative emesse dalla U.O. Tecnologie Informatiche e Telematiche.

2. SEZIONE II – Credenziali

2.1. Le credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete, ai PC ed alle applicazioni, vengono assegnate dal personale dell'U.O. Tecnologie Informatiche e Telematiche, previa formale richiesta del Responsabile dell'Unità Operativa o degli operatori con incarico funzionale, nell'ambito nella quale è inserito o opera l'incaricato.

Le richieste di credenziali devono essere inoltrate dal responsabile attraverso l'apposito sistema informatico di richiesta delle credenziali. La richiesta deve contenere l'elenco delle applicazioni con i rispettivi profili autorizzati.

Le U.O. che gestiscono il trattamento giuridico ed economico del personale sono tenute a comunicare all'U.O. Tecnologie Informatiche e Telematiche, l'attivazione e la cessazione del rapporto di lavoro, nonché l'eventuale trasferimento ad altro servizio e/o mansione del dipendente/collaboratore. La comunicazione può avvenire anche con modalità automatiche.

Le credenziali di autenticazione vengono disattivate dopo 6 mesi di mancato utilizzo, eccetto quelle preventivamente autorizzate per scopi di gestione tecnica.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (nome utente) assegnato dall'U.O. Tecnologie Informatiche e Telematiche, associato ad una parola chiave (password) riservata, che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. In tal senso costituiscono lo strumento di associazione dell'utente con le operazioni svolte. In particolare il nome utente e la password costituiscono una firma elettronica che, in assenza di denuncia di smarrimento o richiesta di blocco, fanno presumere che le attività svolte con tale utenza siano riconducibili all'assegnatario.

In via del tutto eccezionale possono essere autorizzate dalla U.O. Tecnologie Informatiche e Telematiche, credenziali non nominative. L'autorizzazione può essere rilasciata solo a seguito di specifica richiesta con esauriva motivazione e solo laddove non sia possibile garantire lo svolgimento di attività essenziali attraverso il normale utilizzo di credenziali nominative.

Tali credenziali devono essere utilizzate esclusivamente per attività accessorie e mai per il diretto accesso ai dati personali. Le credenziali non nominative sono comunque assegnate ad una persona fisica che sarà responsabile della modalità di utilizzo delle stesse.

2.2. Le password

Le password, quale metodo di autenticazione assegnato dall'Azienda, hanno lo scopo di garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata a soggetti non autorizzati. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Azienda nel suo complesso.

Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza e comunque ogni qualvolta si ritiene che la stessa abbia perso la caratteristica di segretezza.

L'Azienda ha implementato alcuni meccanismi che permettono di aiutare e supportare gli utenti autorizzati in una corretta gestione delle password definendo, laddove tecnicamente possibile, una lunghezza minima delle password, la loro complessità e le politiche di cambiamento delle stesse in funzione di quanto richiesto dalle normative vigenti.

È vietato trascrivere o memorizzare la password su supporti facilmente intercettabili da altre persone.

In qualsiasi momento, per motivi tecnici o di sicurezza, l'Azienda si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo il nome utente o modificando/cancellando la password ad esso associata.

In particolare la password relativa ad un sistema può essere reimpostata dagli amministratori di sistema per le seguenti esigenze:

- Richiesta dell'utente per smarrimento della password
- Rischio imminente di compromissione dei dati per attacco informatico
- Richiesta dell'autorità giudiziaria
- Interventi urgenti a protezione della rete aziendale e del funzionamento dei sistemi

2.3. Regole per la corretta gestione delle password

L'Incaricato, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Obbligo di sostituire la password assegnata al primo accesso;
1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre sostituire immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura" indipendentemente dalla data dell'ultimo cambio;
3. Le password devono essere lunghe almeno 8 caratteri e devono soddisfare almeno 3 dei seguenti requisiti: contenere lettere minuscole, maiuscole, caratteri speciali (ad esempio: { } [] , . < > ; : ! " £ \$ % & / () = ? A \ | ` * - + _) e numeri.
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno ogni 90 giorni a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
6. E' vietato digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Azienda;
7. In alcuni casi, sono implementati meccanismi che consentono all'incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato;
8. La password ideale quindi deve essere complessa, senza alcun riferimento, ma facile da ricordare.

Al fine di una corretta gestione delle password, l'Azienda stabilisce il divieto di utilizzare come propria password:

1. Nome e/o cognome e loro parti;
2. Lo username assegnato;

3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, password e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri o numeri (es. abcabcabc 123456);
8. Password già impiegate in precedenza.

Con specifica procedura operativa la U.O. Tecnologie informatiche e telematiche può modificare le regole tecniche di cui al presente articolo per aggiornarle all'evoluzione tecnologica.

3. SEZIONE III - Operazioni a protezione della postazione di lavoro

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1. Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato si autentica all'interno della propria postazione di lavoro e si connette al sistema informatico aziendale o ad una parte di esso, dichiarando il proprio nome utente e password, aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, intranet), ognuno dei quali richiede un username e una password.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine dell'attività, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa.

3.2. Obblighi

L'utilizzo dei dispositivi assegnati e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve eseguire le operazioni seguenti:

1. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione o in caso di prolungato inutilizzo dello stesso, preferibilmente impostando il logout automatico del Sistema Operativo;
2. Chiudere la sessione (Logout) alla fine del proprio turno di lavoro;
3. Spegnerne il dispositivi dopo il Logout;
4. Controllare sempre che non vi siano persone non autorizzate che possano prendere visione delle schermate del dispositivo (soprattutto all'atto dell'inserimento delle password).

Le politiche di sicurezza aziendali prevedono comunque, dove possibile, la disattivazione automatica della sessione (blocco del dispositivi) dopo un determinato intervallo di inattività.

4. SEZIONE IV – Uso dei dispositivi dell’Azienda

4.1. Modalità d’uso del computer aziendale

Il sistema informatico aziendale è composto da un insieme di unità server centrali e macchine client connesse o meno alla rete aziendale, comunque messe a disposizione dall’Azienda agli Incaricati per lo svolgimento dei compiti affidati e che utilizzano diversi sistemi operativi e applicativi.

I file creati, elaborati o modificati sul dispositivo assegnato e di cui risulta necessario assicurare l’integrità dei dati in caso di rottura del dispositivo stesso, devono essere salvati sui server messi a disposizione dall’Azienda.

L’Azienda non effettua il backup dei dati memorizzati in locale.

Le cartelle utenti presenti nei server dell’Azienda 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 legato all’attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato dell’assistenza tecnica dell’U.O. Tecnologie Informatiche e Telematiche. Tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizionati sui server o copiati sugli stessi periodicamente.

Il personale dell’assistenza tecnica dell’U.O. Tecnologie Informatiche e Telematiche può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità (almeno ogni mese), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un’archiviazione ridondante in ossequio al principio della minimizzazione del trattamento dei dati.

Non è consentito utilizzare aree di scambio per inviare/ricevere file se non autorizzate dall’U.O. Tecnologie Informatiche e Telematiche e se non protette in lettura/scrittura con le opportune credenziali di accesso.

4.2. Corretto utilizzo del computer aziendale

Il dispositivo consegnato all’incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all’attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L’accesso all’elaboratore è protetto da password che deve essere custodita dall’incaricato con la massima diligenza e non divulgata.

Gli addetti all’assistenza tecnica informatica potranno accedere ai computer anche in remoto per attività di manutenzione ed assistenza, previo esplicito consenso del dipendente.

In particolare l'Incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di archiviazione dati messe a disposizione dall'Azienda;
2. In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password inserita. Al fine di evitare che persone non autorizzate effettuino accessi non permessi, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando i tasti CTRL+ALT+CANC);
3. Spegnerne il computer, o curarsi di effettuare il Logout in caso di assenze prolungate;
4. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, chiavette USB), assegnati dall'Azienda;
5. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui si condivide l'utilizzo dello stesso computer o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Divieti espressi sull'utilizzo dei computer

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative, sui dispositivi aziendali;
2. Modificare le configurazioni già impostate sul personal computer;
3. Utilizzare e/o installare programmi e/o sistemi senza la preventiva autorizzazione della U.O. Tecnologie Informatiche e Telematiche;
4. Installare alcun software, né alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale;
5. Caricare sui dispositivi di memorizzazione messi a disposizione dall'Azienda alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Azienda;
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Azienda, quali per esempio virus, malware, trojan horses ecc. ;
8. Accedere, rivelare o utilizzare informazioni per le quali non si è autorizzati o comunque non necessarie per le mansioni svolte;
9. Effettuare in proprio attività manutentive;
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati

dalla U.O. Tecnologie Informatiche e Telematiche;

11. Utilizzare dispositivi di memorizzazione messi a disposizione dell'Azienda su dispositivi non aziendali.

4.4. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, file sharing, chat ecc.

L'Azienda impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L'incaricato, da parte sua, deve rispettare le regole seguenti:

1. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Azienda;
2. Porre massima attenzione all'e mail di dubbia provenienza evitando di aprirne gli allegati e segnalarle tempestivamente all'assistenza tecnica dell'U.O. Tecnologie Informatiche e Telematiche;
3. Non utilizzare chiavette USB personali sui personal computer aziendali in quanto possono essere veicolo di virus che vengono così introdotti nella rete aziendale.

E' necessario contattare l'assistenza tecnica dell'U.O. Tecnologie Informatiche e Telematiche prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra ed anche qualora si sospetti che il dispositivo assegnato risulti infettato da un virus informatico (ad esempio perché presenta un comportamento anomalo).

5. SEZIONE V – Rete locale aziendale

La rete aziendale è una risorsa a disposizione di tutti gli utenti ed è un'infrastruttura critica per l'erogazione di tutti i servizi informatici e di telecomunicazione (compresa la telefonia fissa).

Un corretto utilizzo di questa risorsa da parte di tutti gli utenti contribuisce al buon funzionamento dei servizi erogati.

Per questo motivo è fatto divieto di collegare alla rete aziendale computer personali o computer non assegnati dal competente servizio aziendale, salvo motivata richiesta da parte del Dirigente responsabile del richiedente ed autorizzazione da parte dell'assistenza tecnica dell'U.O. Tecnologie Informatiche e Telematiche.

6. SEZIONE VI – Internet

6.1. Internet è uno strumento di lavoro

La connessione alla rete internet dai dispositivi in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa.

6.2. Misure preventive per ridurre navigazioni illecite

L'Azienda adotta idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list (liste di siti vietati), gli incaricati sono comunque tenuti a rispettare i divieti di cui al successivo art. 6.3.

6.3. Divieti espressi concernenti Internet

E' fatto espresso divieto all'incaricato:

1. di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile;
2. di salvare o installare sul proprio dispositivo programmi o archivi informatici (anche gratuiti) prelevati da siti internet o da strumenti peer to peer;
3. l'utilizzo di dispositivi personali di accesso alla rete quali modem, router 3G/4G/5G ecc. se non nei casi espressamente e formalmente autorizzati dall'U.O. Tecnologie Informatiche e Telematiche;
4. l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line, mining di cripto valuta e simili, salvo i casi autorizzati dall'Azienda, nel rispetto delle procedure di legge;
5. ogni forma di registrazione e accesso a siti i cui contenuti non siano legati all'attività lavorativa;
6. l'utilizzo dei social network, se non espressamente autorizzati, la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Ente, salvo specifica autorizzazione dell'Ente stesso;
7. la navigazione nei siti con contenuti pornografici e pedo-pornografici. È vietata la navigazione nei siti di giochi online;
8. la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
9. accedere dall'esterno alla rete interna dell'Azienda, se non mediante l'utilizzo delle specifiche procedure autorizzate dall'Azienda stessa;
10. creare siti web personali sui sistemi dell'Azienda;

11. acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

L'Azienda al fine di rinforzare tali divieti utilizza degli strumenti informatici a protezione delle risorse aziendali.

Ogni eventuale utilizzo illegittimo di Internet è posto sotto la personale responsabilità dell'Incaricato inadempiente. A seguito di ripetute e significative anomalie, l'Azienda può svolgere verifiche sui dati inerenti l'accesso alla rete dei propri dipendenti. Le navigazioni saranno tracciate e conservate per il tempo strettamente limitato al perseguimento delle suddette finalità.

6.4. Divieti di manomissione dei sistemi di sicurezza

È vietato accedere ai siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Azienda per bloccare accessi non conformi. In ogni caso è vietato bypassare tali filtri o utilizzare software o altri strumenti che consentano la navigazione anonima.

6.5. Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 245). In particolare, è vietato il download di materiale soggetto a copyright (software, testi, immagini, musica, filmati, file in genere).

7. SEZIONE VII – Posta elettronica

7.1. La Posta Elettronica

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. È fatto divieto di utilizzare le caselle di posta elettronica aziendali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- L'invio e/o il ricevimento di allegati contenenti fotografie, filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- L'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, catene telematiche, ecc. non legati all'attività lavorativa;
- L'invio di dati particolari (sensibili), Es. dati sanitari.

In caso di necessità di invio, per esigenze lavorative, di dati sensibili attraverso la posta elettronica tali dati devono essere cifrati tramite apposite chiavi di cifratura fornite dall'U.O. Tecnologie Informatiche e Telematiche e la chiave di decifrazione deve essere comunicata al destinatario, attraverso un altro canale (es: telefono o sms).

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.

Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile contattare il supporto informatico per una ulteriore verifica. Ciò al fine di evitare infezioni da virus, compromissione della propria postazione di lavoro, perdita di dati sensibili, ecc.

Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi, questo per evitare l'infezione da virus informatici.

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto del Servizio di appartenenza. Tale funzionalità deve essere attivata dall'utente.

Gli Incaricati, di norma, hanno in utilizzo indirizzi nominativi di posta elettronica strutturati con il format: **nome.cognome@uslumbria1.it**

Le caselle e-mail possono essere assegnate con natura impersonale (con nomenclatura del tipo: info, amministrazione, fornitori, direttore, direttore sanitario). La nomenclatura sarà attribuita d'ufficio dall'U.O. Tecnologie Informatiche e Telematiche su richiesta degli interessati e sulla base della destinazione di utilizzo della casella. Queste caselle impersonali saranno in ogni caso assegnate ad una persona fisica, che sarà anche responsabile del corretto utilizzo delle stesse.

7.2. Divieti espressi

E' espressamente vietato:

1. Comunicare le proprie informazioni personali o codici di accesso (nome utente e password) in risposta a richieste pervenute via e-mail (phishing);
2. Utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Azienda per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Azienda, nonché utilizzare il dominio dell'Azienda per scopi personali;
3. Creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale;
4. Trasmettere messaggi a tutti i dipendenti senza specifica autorizzazione della Direzione Generale;
5. Sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al

lavoro;

6. Simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi;
7. Inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.

7.3. Posta Elettronica in caso di assenze o cessazione

Ciascun assegnatario di un account di posta elettronica aziendale, dovrà, in caso di assenza prolungata dal servizio, attivare la funzione di risposta automatica presente nel programma di gestione della posta elettronica aziendale.

In tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'assegnatario deve richiedere alla UO Tecnologie Informatiche e Telematiche la configurazione dell'inoltro automatico ad altra casella di posta elettronica aziendale.

In caso di cessazione del rapporto di lavoro o contrattuale con l'Azienda, la casella di posta verrà immediatamente disattivata. La casella verrà eliminata (compresi tutti i messaggi in essa contenuti) entro 6 mesi dalla data della cessazione del rapporto di lavoro.

Eventuali dati personali contenuti nei messaggi di posta elettronica vanno salvati dall'utente prima della cessazione del rapporto di lavoro.

In caso di prolungata assenza imprevista o imprevedibile dell'Incaricato, (per indifferibili esigenze esclusivamente correlate alla attività lavorativa), l'Azienda potrà accedere alla casella di posta elettronica dell'incaricato solo qualora sia stata preventivamente rilasciata formale autorizzazione e nominato un fiduciario da parte dello stesso.

L'eventuale richiesta di accesso alla casella di posta elettronica dell'Incaricato, in caso di assenza prolungata ed imprevista e per documentate ed urgenti esigenze lavorative, deve essere fatta dal Responsabile dell'Incaricato al fiduciario.

Dell'accesso, che deve essere fatto in presenza del fiduciario, deve essere redatto un verbale che deve essere controfirmato da un amministratore di sistema (che attesta che l'accesso è stato effettuato nei termini richiesti) e dal fiduciario. Copia del verbale viene trasmessa all'Incaricato.

8. SEZIONE VIII - Uso di altri dispositivi (personal computer portatile, tablet, cellulare, smartphone ed altri dispositivi elettronici)

8.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dall'Azienda agli Incaricati che durante gli spostamenti necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Azienda.

L'Incaricato è responsabile dei dispositivi mobili assegnatigli dall' Azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, non lasciarlo incustodito o a vista dentro l'auto.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete e comunque tutte le policy di sicurezza previste dall'Azienda.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

L'incaricato dovrà provvedere a trasferire tutti i files creati o modificati sui dispositivi mobili sulle memorie di massa aziendali al rientro in ufficio e cancellarli in modo definitivo dai dispositivi mobili. Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Azienda. In caso di smarrimento o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Azienda che provvederà - se del caso - ad occuparsi delle procedure connesse alla tutela dei dati.

L'incaricato è tenuto comunque alla rimozione di eventuali file elaborati sui dispositivi mobili prima della riconsegna del bene.

8.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Di norma non devono essere utilizzate memorie esterne.

Agli Incaricati può essere assegnata una memoria esterna solo in casi di effettiva e motivata necessità.

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

1. I supporti di memorizzazione rimovibili contenenti dati sensibili o giudiziari, se non più utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri utenti, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
2. I supporti di memorizzazione rimovibili contenenti dati sensibili e/o giudiziari devono essere custoditi in idonei archivi chiusi a chiave, a cura dell'utente che li gestisce abitualmente, e sotto sua diretta ed esclusiva responsabilità.
3. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Qualora le memorie esterne contengano dati particolari (sensibili) e tali memorie esterne vengano portate all'esterno dell'Azienda è responsabilità dell'incaricato cifrare il contenuto della memoria stessa in maniera tale che lo smarrimento accidentale della memoria non comporti la perdita dei dati in essa contenuti.

8.3. Dispositivi personali

E' vietato l'utilizzo e il collegamento a dispositivi aziendali di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet,...).

Ai dipendenti non è permesso svolgere la loro attività lavorativa con strumentazione personale (PC fissi, portatili, tablet, smartphone) in particolare se viene connessa alla rete aziendale.

Gli Incaricati non dipendenti (ovvero i consulenti, collaboratori esterni e fornitori), possono utilizzare i propri dispositivi personali per memorizzare dati inerenti l'attività dell'Azienda solo se espressamente autorizzati dall'U.O. Tecnologie Informatiche e telematiche e assumendo formalmente e personalmente la responsabilità dei trattamenti svolti.

Tali dispositivi dovranno essere preventivamente valutati per la verifica della sussistenza di misure minime ed idonee di sicurezza.

8.4. Distruzione dei Dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Azienda che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'Azienda provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

E' responsabilità dell'incaricato salvare eventuali dati personali contenuti nel dispositivo prima della riconsegna dello stesso all'U.O. Tecnologie Informatiche e Telematiche. L'Azienda non potrà essere ritenuta responsabile per la perdita di dati personali contenuti in dispositivi aziendali.

9. SEZIONE IX – Sistemi in cloud

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Azienda a potenziali problemi di violazione delle regole sulla riservatezza dei dati personali.

E' vietato agli incaricati l'utilizzo di sistemi cloud (es. Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, etc.) non espressamente approvati dall'Azienda, in particolare è vietato condividere o registrare su sistemi cloud dati sanitari.

L'Azienda si riserva di identificare tecnologie e/o servizi cloud conformi alla normativa in materia di trattamento dei dati personali, da mettere a disposizione degli Incaricati.

10. SEZIONE X – Accesso autorizzato dall'esterno mediante VPN

L'Azienda permette di accedere alla propria infrastruttura tecnologica, mediante canali di comunicazione protetti **VPN** (*Virtual Private Network*), a determinate categorie di utenti previa valutazione della richiesta e/o di accordi contrattuali.

Per accedere all'infrastruttura, ogni Utente VPN per ottenere le credenziali/abilitazioni necessarie, dovrà compilare in ogni sua parte e sottoscrivere un modulo messo a disposizione dalla UO Tecnologie Informatiche e Telematiche. Lo stesso modulo dovrà essere validato per l'autorizzazione dal proprio Dirigente di struttura.

In particolare dovranno essere specificate le motivazioni per le quali si può richiedere un accesso dall'esterno in VPN:

- reperibilità tecnica
- firma atti (dirigenti apicali)
- personale in telelavoro
- attività sanitarie effettuabili a distanza specificamente autorizzate dal Direttore Sanitario (a titolo di esempio: aggiustamento terapia anticoagulante, refertazione radiologica in reperibilità)

Possono accedere all'infrastruttura tecnologica tramite VPN gli utenti a cui sono state assegnate le credenziali di accesso personali, esclusivamente per il periodo di tempo necessario all'espletamento dei propri compiti.

11. SEZIONE XI – Applicazione e controllo

11.1. Il controllo

L'Azienda, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni, in conformità alla vigente normativa per le seguenti finalità:

1. Garantire il funzionamento dei sistemi e dei servizi informatici e di telecomunicazioni
2. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
3. Evitare che siano commessi illeciti o per esigenze di carattere difensivo anche preventivo;
4. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire tramite monitoraggio, audit e/o ispezioni del sistema informatico e di tutti i dispositivi aziendali o comunque collegati alla rete aziendale. Per tali controlli l'Azienda si riserva di avvalersi anche di soggetti esterni.

Tutti i controlli saranno effettuati in conformità alla normativa vigente con particolare riferimento alla normativa in materia di trattamento dei dati e dello Statuto dei Lavoratori.

11.2. Modalità di verifica

Le attività sull'uso del servizio di accesso a internet e in generale dei servizi informatici più critici sono automaticamente conservate in registri informatici (comunemente chiamati file di LOG) che possono riportare dettagli della navigazione, dei siti, dei documenti consultati e le operazioni che si sono verificate.

I file di log contengono tipicamente:

- Data ed ora dell'operazione effettuata
- Utente che ha effettuato l'operazione
- Tipologia dell'operazione effettuata
- Dati associati all'operazione effettuata

In applicazione di quanto previsto dall'art. 5 del Regolamento Generale Sulla Protezione Dei Dati (GDPR), l'Azienda promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Incaricati e a tale scopo adotta, compatibilmente con le risorse disponibili, strumenti tecnici, organizzativi e fisici, volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Azienda non adotta sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora venga rilevato un non corretto utilizzo degli strumenti informatici messi a disposizione dall'Azienda da parte degli utenti, si procederà all'invio di un avviso all'utente ed al Responsabile del Servizio interessato. Sarà cura del Responsabile del Servizio interessato segnalare eventualmente l'evento all'Ufficio per i procedimenti disciplinari per l'adozione degli atti di rispettiva competenza. Per il personale Dirigente il comportamento verrà comunicato alla Direzione Aziendale.

11.3. Modalità di conservazione

I sistemi software sono stati programmati e configurati in modo da registrare nei LOG di sistema i dati relativi agli accessi ad internet, al traffico telematico ed alle operazioni effettuate sui sistemi informatici più critici per un arco temporale la cui durata è riportata nel registro dei trattamenti, in funzione delle caratteristiche tecniche degli apparati e dei sistemi disponibili.

Possono essere implementati tempi di conservazione più lunghi in relazione a:

1. esigenze tecniche o di sicurezza, valutate a cura dell'U.O. Tecnologie Informatiche e Telematiche e documentate in forma scritta;
2. indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate e sarà effettuato con logiche e forme strettamente correlate agli obblighi, compiti e finalità già esplicitati.

L'accesso ai dati avviene attraverso le figure tecniche istituzionalmente autorizzate ed in possesso delle opportune credenziali di accesso (a titolo esemplificativo: amministratori di sistema, tecnici di società esterne titolari di contratti per servizi di assistenza e manutenzione).

12. SEZIONE XII – Validità e pubblicazione

12.1. Validità

Il presente Disciplinare ha validità a decorrere dalla data stabilita nella Delibera di adozione del Direttore Generale.

Con l'entrata in vigore del presente disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Copia del Disciplinare sarà pubblicata sulla rete Intranet aziendale.

L'Azienda promuove la conoscenza del presente Disciplinare da parte degli incaricati anche tramite apposite sessioni di formazione.

12.2. Pubblicazione

Il presente Disciplinare verrà diffuso a tutti i dipendenti mediante pubblicazione sulla intranet aziendale.