SERVIZIO SANITARIO NAZIONALE - REGIONE BASILICATA

azienda sanitaria locale
matera

REGOLAMENTO
PER L'UTILIZZO DELLE RISORSE INFORMATICHE, DELLA RETE INTERNET E DELLA TELEFONIA.

INDICE

1. PREMESSA 3
2. OGGETTO E CAMPO DI APPLICAZIONE 4
3. UTILIZZO DEL PERSONAL COMPUTER 5
4. UTILIZZO DI PC PORTATILI 8
5. GESTIONE DEL SERVIZIO 9
6. PROCEDURE ANTIVIRUS 9
7. BACKUP E PULIZIA 10
8. UTILIZZO DELLA RETE 10
   8.1 PERIFERICHE E CARTELLE CONDIVISE 11
9. UTILIZZO DI INTERNET E RELATIVI SERVIZI 12
10 UTILIZZO DELLA POSTA ELETTRONICA 13
   10.1 MANUTENZIONE DELLA CASELLA DI POSTA 15
11 UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA (P.E.C.) 15
12 UTILIZZO DEI SERVIZI DI TELEFONIA FISSA E MOBILE 16
12 MODALITA' GENERALI DI CONTROLLO 17
13 SANZIONI 18
14 REVISIONE E AGGIORNAMENTI 18
15 INFORMATIVA AI SENSI DELL' ART 13 REGOLAMENTO UE 679/2016 18
16 NORMATIVA DI RIFERIMENTO 18

1. PREMESSA

Il presente documento è redatto secondo quanto disposto dal Garante per la Protezione dei dati personali nel provvedimento a carattere generale del 01/03/2007, che prescrive ai datori di lavoro privati e pubblici di adottare le misure necessarie a garanzia degli interessati, riguardante l'onere di specificare le modalità di utilizzo della rete intranet, della posta elettronica e di internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati i controlli. Con tale provvedimento, il Garante indica altresì ai medesimi datori di lavoro, a garanzia degli interessati, il rispetto di alcune linee guida, tra cui l'adozione e la pubblicizzazione di un disciplinare interno oltre che l'adozione di misure di tipo organizzativo e tecnologico afferenti alla navigazione in internet e all'utilizzo della posta elettronica.

Per i servizi di telefonia, si richiamano altresì la Circolare del Ministero della Funzione Pubblica n. 6/96 del 13.03.96, la direttiva della PCM del 20.07.99 e la Direttiva del Ministero dell'Innovazione del 30.10.2001.

Il presente Regolamento è adottato al fine di indicare le misure necessarie ed opportune per il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), dei dispositivi elettronici aziendali in generale (tablet, smartphone, ecc.), della posta elettronica e di internet, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura della sicurezza informatica.

Premesso che, l'utilizzo delle risorse informatiche, telematiche e telefoniche deve sempre ispirarsi al principio della diligenza e della correttezza nonché dell'appropriatezza d'uso, comportamenti normalmente adottati nell'ambito dei rapporti di lavoro, l'Azienda adotta il presente regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e nella condivisione delle risorse. Infatti la progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra i computer e l'aumento delle informazioni trattate con strumenti elettronici determinano la crescita dei rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

L'utilizzo dei servizi informatici e delle relative risorse di rete deve avvenire:

- Nel rispetto delle leggi e delle norme vigenti ed in particolare delle leggi in materia di sicurezza, privacy, copyright, accesso ed uso dei sistemi informatici e telematici;
- Nel rispetto delle norme e procedure lavorative generali definite dall'Azienda, nel riguardo dei diritti degli altri utenti e dei terzi.

Il controllo del corretto utilizzo degli strumenti ed in generale del rispetto del presente regolamento da parte dei lavoratori deve avvenire nel rispetto dei diritti alla riservatezza e alla dignità degli operatori stessi, come sancito dalla L. 300/1970 (cd. Statuto dei lavoratori), recentemente modificato a seguito del Jobs Act,

nonché della Normativa in materia di protezione dei dati personali.

Per le medesime finalità è altresì disciplinato l'utilizzo dei servizi di telefonia.

L'Azienda deve provvedere a garantire un servizio continuativo, nel suo stesso interesse, ed assicurare la riservatezza delle informazioni e dei dati elaborati, in modo da evitare che comportamenti inconsapevoli (quando non irresponsabili) possano innescare e/o determinare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche.

Ferme restando le disposizioni normative in materia e tutte le prescrizioni previste per il trattamento dei dati particolari o giudiziari, il contenuto del presente Regolamento interno costituisce disposizione di servizio e viene notificato a tutti gli utilizzatori attuali e potenziali mediante pubblicazione sul sito istituzionale dell'Azienda.

2. OGGETTO E CAMPO DI APPLICAZIONE

Il presente Regolamento contiene le disposizioni relative alle corrette modalità di utilizzo della rete informatica dell'Azienda e di tutte le risorse informatiche e telefoniche, in conformità e nel rispetto di quanto previsto dalla specifica normativa di settore e dalle ulteriori disposizioni emanate dall'Azienda.

Per risorse informatiche si intendono tutti i servizi e gli apparati di proprietà dell'Azienda messi a disposizione dei dipendenti per permettere il normale svolgimento delle proprie prestazioni lavorative o attivati per la tutela delle persone o del patrimonio aziendale . Tali risorse sono individuabili nei computer, nei sistemi di identificazione e di autenticazione informatica, nell'uso di internet e negli strumenti per lo scambio di comunicazioni e file, nella posta elettronica e in qualsiasi altro programma e/o apparecchiatura informatica destinata ad elaborare, memorizzare o trasmettere dati e informazioni, nonché impianti di videosorveglianza.

Per servizi di telefonia si intende l'impiego di tutti gli apparecchi di telefonia fissa e mobile e telefax a prescindere che siano collegati o meno a centrali telefoniche nonché dal tipo di abilitazione impostata.

Tutti i soggetti che utilizzano gli strumenti informatici, telematici e telefonici messi a disposizione dall'Azienda hanno la responsabilità di applicare e rispettare puntualmente le disposizioni del presente Regolamento.

Il Regolamento si applica a tutto il personale dipendente dell'Azienda, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori a prescindere dal rapporto contrattuale con la stessa intrattenuto (liberi professionisti, collaboratori a progetto, stagisti e borsisti, ecc.).

Sono esentati dall'applicazione del presente Regolamento, solo limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema.

3. UTILIZZO DEL PERSONAL COMPUTER

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare e/o determinare disservizi, costi di manutenzione e/o di ripristino, danni, e, soprattutto, minacce alla sicurezza. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Dirigente/Responsabile diretto.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza, evitando la sua divulgazione. Le password (autenticazione pc, eMail, P.E.C. ecc.) devono essere utilizzate per l'accesso alla rete e per l'accesso a qualsiasi applicazione che lo preveda.

L'attivazione e/o la modifica della password di accensione del personal computer (BIOS) è consentita solo all'amministratore di sistema.

Le password utilizzate devono contenere almeno 8 caratteri, non devono contenere riferimenti, diretti o indiretti, agevolmente riconducibili all'incaricato e devono utilizzarsi preferibilmente anche caratteri speciali e lettere maiuscole e minuscole. Le parole chiavi devono essere custodite con la massima attenzione e segretezza e non devono essere divulgate o comunicate a terzi. L' utente è responsabile di ogni utilizzo indebito o non consentito delle parole chiavi di cui sia titolare.

Qualora, in caso di prolungata assenza o impedimento dell' utente, ci sia la necessità di accedere ai dati ed agli strumenti elettronici per esclusive necessità di servizio e/o di sicurezza del sistema, il responsabile della struttura chiede all'amministratore di sistema che ne ha la funzione di provvedere al prelievo di quanto richiesto. Al rientro in servizio dell'incaricato assente ovvero impedito, il responsabile della struttura provvederà ad informarlo dell'accaduto.

Ogni utente che necessita di accedere a file/applicazioni deve essere dotato di credenziali di autenticazione nominative non condivisibili.

Se l'incaricato ritiene che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della password, in autonomia. Il dipendente, si impegna a:

- non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- non lasciare incustodita ed accessibile la propria postazione una volta che sia avvenuta l'autenticazione con le proprie credenziali;
- conservare e custodire le password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (nome utente e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti casualmente a conoscenza;

- mantenere la corretta configurazione del proprio elaboratore non alterando le componenti hardware e software predisposte né installando ulteriori software non autorizzati.

Qualunque azione o attività esercitata mediante l'utilizzo del codice identificativo e della password assegnati, è ascritta in via esclusiva all'utente assegnatario delle credenziali di autenticazione che sarà chiamato a rispondere delle attività eseguite. L'utente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua parola chiave, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico e il buon costume così come definiti dalla giurisprudenza più recente. La violazione delle presenti disposizioni può comportare l'applicazione delle sanzioni disciplinari previste dai vigenti Contratti Collettivi di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

In assenza di un elenco di programmi installabili, già autorizzati dall'Azienda, non è consentito installare autonomamente e/o mandare in esecuzione programmi provenienti dall'esterno o scaricati da internet senza la preventiva autorizzazione dell'Amministratore di Sistema, sentito il responsabile della struttura competente. E' assolutamente vietato installare, anche solo temporaneamente, programmi ottenuti o sbloccati illegalmente (programmi crackati, codici di sblocco ottenuti da internet, etc.).

Non è consentita la disinstallazione dei programmi, sia software di base che software applicativi presenti sui computer assegnati agli utenti.

I suddetti interventi sono effettuati, in caso di necessità, solo a cura dei tecnici preposti dietro motivata richiesta dell'utente.

L'utente è responsabile del software installato sul proprio PC, sia software di base che software applicativo di vario genere (es. software di gestione del personale, database di archiviazione dati, etc.) e del suo corretto utilizzo; se ne raccomanda pertanto un uso diligente.

Non è consentita l'installazione, anche se necessaria, di eventuali driver per stampanti o altri supporti come ad esempio masterizzatori, scanner, etc.; in questo caso l'utente dovrà richiedere ai tecnici preposti di intervenire per effettuarne l'installazione.

In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente ad alcune aree tematiche, deve essere comunque richiesto il parere degli Amministratori di Sistema, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Ciò al fine di scongiurare il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni già installate con dispendio di tempo, di risorse, di rischio di perdita di dati, di sovraccarico della rete locale, con degrado delle prestazioni per gli altri utenti connessi in rete, di sovraccarico dei collegamenti sulla rete internet, con degrado delle prestazioni per gli altri utenti e violazione della normativa a tutela dei diritti d'autore (D.lgs. 518/92 e L. 248/2000) che impone l'utilizzo di software libero o di software proprietario munito di regolare licenza.

Non è consentito all'utente modificare le configurazioni di sistema impostate sui PC assegnati, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del/i browser per la navigazione, né utilizzare in modo improprio e/o cedere il proprio indirizzo di rete ad altri utenti e/o spostarlo indebitamente su altre apparecchiature (pc, notebook, tablet, smartphone, ecc.). Ogni Dirigente/Responsabile ha l'obbligo di verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi dei punti di rete in luoghi non presidiati.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In difetto, il comportamento del dipendente si configura come negligente, inescusabile e gravemente colposo. Qualora ci si allontani dalla propria postazione occorre disconnettersi o bloccare il personal computer (per il sistema operativo Windows premendo contemporaneamente i tasti Alt+Ctrl+Canc e cliccare su "Blocca computer" oppure tasto bandierina [icona Windows] + L).

Inoltre:

- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali Dropbox, Google drive, Microsoft one drive, Mega, ed in generale tutti i software che ricadono nella categoria "cloud storage", software VPN, software di assistenza remota);
- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte degli Amministratori di Sistema (quali DNS, DHCP, server Web, FTP,…);
- non è consentito intercettare pacchetti sulla rete (sniffing) o utilizzare software dedicati a carpire, in maniera invisibile, dati personali, password e userID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dagli Amministratori di Sistema incluse versioni live su CD Rom /Dvd e/o pendrive Usb;
- non è consentito utilizzare connessioni in remoto per l'accesso a risorse di Azienda, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate e autorizzate da parte degli Amministratori di Sistema;
- non è consentito il collegamento al proprio PC o la connessione alla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili, telefoni cellulari ed altri apparati in genere).

Agli utenti che trattano dati particolari o giudiziari è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (Penne USB, CD-Rom, ecc.) una volta che non sia possibile rendere irrecuperabili i dati in essi contenuti. Ai sensi della normativa vigente è fatto divieto di divulgazione a

qualsiasi titolo delle informazioni presenti nelle banche dati dell'Ente se non disciplinate da appositi protocolli di intesa e/o da autorizzazioni specifiche.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente gli Amministratori di Sistema nel caso in cui, all'atto del loro uso, siano rilevati virus ed adottando quanto previsto dal successivo articolo 6 del presente Regolamento relativamente 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. Per nessun motivo la postazione di lavoro assegnata all'utente può essere aperta e/o manipolata, né nel caso di presunto guasto hardware né per qualsiasi altra motivazione, neppure per scambiare semplicemente tra un PC ed un l'altro qualsiasi apparecchiatura in dotazione all'utente. L'apertura, la manipolazione, la sottrazione di parti di essa (hard disk, memoria RAM, schede di interfacciamento, etc.) è segnalato da parte dell'Amministratore di Sistema al Dirigente/Responsabile a cui la risorsa è assegnata, ai fini della contestazione dell'addebito e del conseguente potenziale procedimento disciplinare.

Il personale è tenuto ad osservare le direttive degli Amministratori di Sistema volte a garantire il corretto funzionamento delle procedure di backup. E' vietato utilizzare gli strumenti informatici al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi privi di regolare licenza) e/o altro materiale non autorizzato. E' vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, files musicali, immagini, filmati e simili) di cui l'Ente non abbia acquisito i diritti.

A tutti gli utenti è espressamente vietato, e costituisce addebito contestabile a fini disciplinari, l'uso di software e hardware atto ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici (es. in conseguenza di attività di sniffing, di spoofing, di creazione di hot spot Wi-Fi, etc.).

Inoltre si precisa che l'assegnazione della risorsa "Personal Computer" non ne comporta la privatezza, in quanto trattasi di strumento di esclusiva proprietà Aziendale.

4. UTILIZZO DI PC PORTATILI

Il dipendente al quale sia stato assegnato dall'Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l'utilizzo sul luogo di lavoro. L'utilizzo del personal computer portatile è soggetto alle stesse regole previste per i personal computer fissi connessi in rete; non è pertanto cedibile a terzi estranei all'Ente e deve essere utilizzato ai soli fini istituzionali. I PC portatili utilizzati all'esterno (convegni, corsi, sopralluoghi etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni e/o sottrazioni/furti.

5. GESTIONE DEL SERVIZIO

Della gestione delle risorse informatiche così come dell'abilitazione per la connessione ad internet è responsabile la struttura dell'ICT Aziendale.

La struttura dell'ICT Aziendale è tenuta a:

- Adottare le misure più idonee a garantire continuità, disponibilità e sicurezza del servizio;
- Gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali;
- Informare tempestivamente e preventivamente gli utenti di eventuali fermi o interruzioni di servizio che si rendessero necessari per manutenzione o per cause di forza maggiore;
- Monitorare i livelli di servizio al fine di garantire la massima efficienza e garantire la funzionalità tecnica;
- L'individuazione delle risorse informatiche (hardware e software) da acquistare ed il collaudo delle stesse;
- La configurazione e l'amministrazione delle risorse informatiche Aziendali e della rete. Per risorse informatiche si intendono: server, workstation, personal computer, notebook, stampanti utilizzati dai dipendenti, amministratori, personale con incarichi professionali, stagisti, tirocinanti ed eventuali ospiti;
- Richiedere l'assistenza per l'attivazione/disattivazione della casella di Posta Elettronica e della P.E.C. per il personale autorizzato.

La struttura dell'ICT Aziendale può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell'Azienda, sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

Vige l'assoluto divieto, al personale della struttura dell'ICT Aziendale, di effettuare controlli con le seguenti modalità:

- La riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- La lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- L'analisi occulta di computer fissi o portatili affidati in uso.

6. PROCEDURE ANTIVIRUS

Ogni utente deve adottare comportamenti tali da ridurre al minimo il rischio di attacchi al sistema informatico aziendale dovuti a virus o altro codice maligno (worm, trojan, DoS, spyware, backdoor, ecc.).

E' buona norma, ad esempio:

- Non aprire mail o relativi allegati sospetti o che contengano un'estensione doppia;

- Non navigare sui siti non professionali;
- Non considerare le icone mostrate dagli allegati come garanzia dell'integrità del software;
- Ogni dispositivo per la memorizzazione di dati (hard disk, dispositivi usb, cd/dvd, ...) dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato;
- In caso di ricezione di una e-mail, non attinente all'attività svolta, da mittenti sconosciuti e/o sospetti, con oggetto/contenuto del messaggio insolito, non aprire né cliccare sui link presenti né aprire eventuali allegati; in generale eliminare immediatamente – senza aprirle - mail non attese e non pertinenti all'attività lavorativa svolta;
- In casi dubbi effettuare un controllo con il mittente prima di aprirne l'eventuale allegato.

Ogni utente è tenuto comunque a controllare la presenza e il regolare aggiornamento del software antivirus e della definizione dei virus. Qualora il software antivirus rilevi la presenza di un malware che non è riuscito ad eliminare, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, scollegare il cavo di rete e segnalare l'accaduto agli Amministratori di Sistema senza effettuare alcuno scambio di dati con altri.

7. BACKUP E PULIZIA

Ogni utente è responsabile della corretta conservazione dei dati e dei documenti elettronici (ad esclusione di quelli prodotti dalle Procedure Informatizzate Aziendali, a titolo esemplificativo e non esaustivo: AIRO, Paghe, Protocollo Informatico, ecc…) che utilizza per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (personal computer fissi e portatili) è demandata all'utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione.

8. UTILIZZO DELLA RETE

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 e funge da mezzo di trasporto per altri tipi di informazioni (ad esempio, telefonia interna, videoconferenza, formazione a distanza, telecontrollo degli apparati, ecc…), 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'Amministratore di Sistema.

- É proibito a chiunque l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto.
- É vietato depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio.
- É vietato calpestare o schiacciare con arredi, sedie ecc., i cavi di collegamento delle postazioni alla rete Lan.
- É obbligatorio interpellare la struttura dell'ICT Aziendale prima di ogni spostamento di postazioni informatiche, per valutarne l'impatto e/o la fattibilità e per predisporre le configurazioni adeguate.

8.1 Periferiche e Cartelle Condivise

Per periferiche condivise si intendono fotocopiatori, stampanti, scanner, plotter o qualsiasi altro dispositivo elettronico che può essere utilizzato contemporaneamente e/o indipendentemente da più utenti.

Per cartella condivisa (unità di rete) si intende uno spazio disco disponibile su un dispositivo di storage di rete (Network Attached Storage - N.A.S) o server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati. L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare in queste aree, anche temporaneamente, qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. L'utente è tenuto, altresì, alla periodica (almeno ogni 6 mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti e/o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua ed uno spreco degli spazi di memorizzazione.

L'utilizzo delle periferiche condivise è riservato esclusivamente a compiti di natura strettamente istituzionale.

I Dirigente/Responsabile diretto si impegnano ad eliminare, ove è possibile, le stampanti e/o gli scanner personali in favore di quelli di rete (condivisi), che permettono un risparmio nei costi di gestione/manutenzione.

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo dei materiali di consumo (toner, cartucce,…);
- prediligere le stampanti laser in luogo di quelle che prevedono costi di gestione maggiori, quali stampanti a getto di inchiostro;

- stampare in bianco/nero e fronte/retro al fine di ridurre i costi, laddove possibile.

Le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro inutilizzo.

9. UTILIZZO DI INTERNET E RELATIVI SERVIZI

L'elaboratore abilitato alla navigazione in internet costituisce uno strumento messo a disposizione dall'Azienda per supportare lo svolgimento della propria attività lavorativa ed è quindi vietata la navigazione in internet per finalità differenti.

Non è consentito agli utenti scaricare da internet software di qualsiasi tipo (freeware, shareware, "crackati" ovvero "sprotetti") né file multimediali (musica, filmati, immagini), né collegarsi a siti che effettuino streaming audio e/o video (per esempio ascolto/visione in tempo reale di una radio o di una tv tramite internet).

Tali attività, oltre a costituire una fonte di potenziali pericoli per la sicurezza del sistema ed un'eventuale violazione dei diritti d'autore, sovraccaricano notevolmente la rete, degradandone le prestazioni e facendo lievitare significativamente i bisogni ed i costi per la trasmissione dati.

- È vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi esplicitamente autorizzati per lo svolgimento dell'attività lavorativa;
- Non è consentita alcuna forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

Non è consentito altresì:

- acquisire e diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
- diffondere prodotti informativi di natura politica, se non espressamente autorizzati da fonti legislative o regolamentari;
- la partecipazione a forum non inerenti l'attività lavorativa, l'utilizzo di social network, chat line, di bacheche elettroniche e le registrazioni in guest books;
- diffondere informazioni riservate di qualsiasi natura;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

A tal fine l'Azienda, di concerto con struttura dell'ICT Aziendale può adottare misure di tipo tecnologico appropriate al fine di:

- individuare categorie di siti considerati correlati o non correlati con la prestazione lavorativa;

- configurare sistemi o filtri che impediscono l'accesso diretto ai siti che non hanno natura istituzionale (black list);
- estrarre informazioni in modalità aggregata e tali da permettere l'analisi del traffico dei dati fornendo informazioni di controllo utili agli amministratori di sistema;
- conservare i dati inerenti il traffico internet per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza.

La navigazione in internet costituisce oggetto di controllo da parte degli amministratori di sistema, nel rispetto dei principi di pertinenza e non eccedenza secondo le modalità indicate nelle Linee Guida del Garante di cui alla Deliberazione n. 13 del 1 marzo 2007. I sistemi software allo scopo predisposti saranno programmati e configurati in modo da cancellare periodicamente i dati relativi agli accessi internet ed al traffico telematico secondo quanto previsto da tali Linee Guida.

10 UTILIZZO DELLA POSTA ELETTRONICA

Per lo svolgimento delle mansioni lavorative, viene attribuita, a tutti i dipendenti che ne facciano richiesta, una casella di posta elettronica aziendale nel formato:

***nome.cognome@asmbasilicata.it*.**

La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione dell'operatore al solo fine dello svolgimento delle proprie mansioni lavorative. Si invitano i dipendenti a non utilizzare gli indirizzi di posta assegnati per comunicazioni personali e si sottolinea che, tranne nel caso di posta elettronica certificata (P.E.C.), le comunicazioni per il tramite della posta elettronica convenzionale **non** sostituiscono le comunicazioni formali.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere, in calce, un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi, del tipo:

"***Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento Aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente***".

Si raccomanda di utilizzare l'email esclusivamente per finalità legate all'attività lavorativa. Si segnala, inoltre, che a meno di utilizzare un indirizzo di posta elettronica certificata con l'apposizione della firma digitale sul documento trasmesso, i sistemi di posta elettronica convenzionale non garantiscono la riservatezza delle informazioni trasmesse; per questo motivo si raccomanda ai dipendenti di non inoltrare,

con tale mezzo, informazioni e dati classificabili come “particolari’ ovvero “giudiziari” ai sensi dell’ art. 4 del Regolamento UE 2016/679.

Possono essere assegnate, qualora si rendesse necessario per esigenze organizzative del lavoro, delle caselle di posta istituzionali (caselle di posta utilizzate da UO/Strutture, ad esempio: urp@asmbasilicata.it)

Nell’effettuare la richiesta dovranno essere elencati i nominativi delle persone autorizzate all’utilizzo della casella di posta istituzionale.

Di seguito si riportano le principali raccomandazioni a cui attenersi:

- l’utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza ed a rispondere in tempi ragionevoli alle email ricevute;
- le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale, devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l’oggetto, in modo tale che il destinatario possa immediatamente individuare l’argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- non superare la dimensione complessiva di 15 Megabyte degli allegati inviati con un solo messaggio ad un singolo indirizzo o complessivamente e contemporaneamente a più destinatari;
- limitare l’invio di messaggi di posta elettronica collettivi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio;
- non inviare messaggi di natura ripetitiva (c.d. catene di Sant’Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Gli utenti devono evitare di contribuire (ancorché in modo inconsapevole) alla diffusione dei virus informatici:

- cancellando immediatamente eventuali messaggi ricevuti da mittenti sconosciuti e/o sospetti e, soprattutto, NON aprendo NÉ eseguendo MAI gli eventuali allegati;
- verificando il contenuto dei messaggi ricevuti e/o trasmessi, soprattutto se contenenti allegati;
- evitando di inoltrare ad altri utenti i messaggi ricevuti, senza averne verificato il contenuto.

Si deve prestare la massima attenzione al contenuto dei messaggi di posta elettronica scambiati con altri utenti (interni/esterni).

In particolare, è tassativamente vietato trasmettere via email:

- materiale che possa essere considerato molesto/osceno, razzista, pedofilo/pornografico o illegale;

- contenuti ingiuriosi o diffamatori che possano comportare eventuali corresponsabilità a carico dell'Azienda e/o impatti negativi sull'immagine della stessa.

Gli utenti devono contribuire alla riduzione del fenomeno "spam" (trasmissione su larga scala e in grandi volumi di eMail non sollecitate):

- evitando di rispondere e/o inviare ad altri utenti gli eventuali messaggi non sollecitati che siano stati ricevuti ed evitando altresì di comunicare ad altri utenti, in modo indiscriminato, il proprio indirizzo di posta elettronica;
- evitando di registrare il proprio indirizzo di posta elettronica sui siti web sospetti e/o mailing list non direttamente correlate alla propria attività lavorativa;
- evitando di inviare messaggi di posta elettronica con allegati di grosse dimensioni a più utenti contemporaneamente;

E' inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali a proprio beneficio e/o di altri.

10.1 Manutenzione Della Casella Di Posta

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga ne saturino lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare anche i messaggi contenenti allegati di grandi dimensioni presenti nelle cartelle POSTA INVIATA, POSTA RICEVUTA; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella POSTA ELIMINATA/CESTINO utilizzando la voce SVUOTA CARTELLA POSTA ELIMINATA/CESTINO.

L'utente può decidere di conservare i messaggi e gli allegati di posta elettronica sul server: in tal caso al fine di non saturare lo spazio disco, è tenuto personalmente ad effettuare periodicamente la manutenzione del contenuto della propria casella di posta provvedendo all'eliminazione dalla mailbox dei messaggi obsoleti o non utili in arrivo ed in partenza e al successivo svuotamento della posta elettronica eliminata.

Nel caso in cui l'utente non provveda ad effettuare la manutenzione della propria casella di posta elettronica aziendale, alla saturazione dello spazio concesso, la mailbox va in blocco e cessa di funzionare, pertanto le nuove eMail non vengono più ricevute dal sistema.

11 UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA (P.E.C.)

Le caselle di posta elettronica certificata (P.E.C.) permettono di trasmettere e di ricevere documenti ufficiali in sostituzione della posta cartacea, certificandone, quindi, l'invio e la ricezione. Tali caselle P.E.C. possono essere associate al sistema di protocollazione elettronico dell'Azienda per assicurarne, tra l'altro, l'interoperabilità tra i protocolli delle PP. AA.

Al fine di favorirne l'utilizzo prioritario, l'Azienda pubblicizza i propri indirizzi P.E.C.: i vari uffici, prima di inviare un documento con le ordinarie modalità di spedizione devono assicurarsi che l'invio non possa avvenire mediante P.E.C.

Per la posta elettronica certificata valgono le stesse raccomandazioni fatte per la posta elettronica convenzionale, con la differenza che gli eventuali allegati inviati non devono superare la dimensione complessiva di 30 Megabyte (limite minimo garantito per legge) con un solo messaggio inviato ad un singolo indirizzo o complessivamente a più destinatari. Per gli assegnatari di casella di posta elettronica certificata, essendo la P.E.C. equivalente alla raccomandata A/R tradizionale, avendone lo stesso valore legale, ovvero l'opponibilità a terzi della spedizione e ricezione di un documento, è **obbligatoria la consultazione tempestiva in modo da evitare pregiudizi o comunque danni all'Ente**. Come per la posta elettronica convenzionale è necessario archiviare/scaricare periodicamente il contenuto delle caselle in modo da evitare che le stesse caselle si possano riempire, rendendo impossibile l'invio e/o la ricezione di nuovi messaggi. In caso di saturazione casella PEC, l'utente si deve rivolgere alla struttura dell'ICT Aziendale.

12 UTILIZZO DEI SERVIZI DI TELEFONIA FISSA E MOBILE

I principi ed i criteri sopra enunciati sono altresì applicati in merito all'utilizzo dei dispositivi e dei servizi di telefonia fissa e mobile.

In particolare, fermi restando tutti gli accorgimenti tecnici e tecnologici per tempo resi disponibili nell'ambito dei servizi e dei dispositivi acquisiti alle migliori condizioni di mercato mediante Consip o altri soggetti aggregatori previsti per legge (VOIP, numeri passanti, etc.), sono qui richiamati e ribaditi i doveri e gli obblighi di utilizzo diligente, corretto ed appropriato dei dispositivi e dei servizi di telefonia fissa e mobile da parte dei dipendenti dell'Azienda e di tutti gli utilizzatori dei detti dispositivi e servizi a qualsiasi titolo, nonché la responsabilità diretta e personale in caso di inosservanza degli stessi.

Gli apparecchi e dispositivi telefonici ovunque ubicati ed assegnati a postazioni di lavoro o funzioni di telefonia o trasmissione dati devono essere utilizzati esclusivamente per l'espletamento dell'attività di servizio. Ciascun responsabile di articolazione organizzativa garantisce che il personale non usi le attrezzature ed i servizi di cui sopra per finalità diverse da quelle istituzionali.

Per le comunicazioni telefoniche tra uffici e/o strutture aziendali collegate in rete, gli utilizzatori sono tenuti ad avvalersi dei numeri diretti interni evitando la comunicazione attraverso la linea telefonica urbana e interurbana.

Le chiamate internazionali devono transitare tramite centralino, salva abilitazione alle chiamate dirette.

E' vietato l'utilizzo di numeri speciali a pagamento.

L’uso di apparecchiature e servizi di telefonia mobile deve essere autorizzato dalla Direzione Aziendale osservando criteri di utilizzazione predeterminati, quali esigenze di reperibilità, servizi fuori sede, interventi prescritti per ragioni di pubblica sicurezza, etc.

L’Amministrazione si riserva il controllo a campione delle telefonate effettuate mediante tabulati appositamente richiesti ai gestori dei servizi di telefonia fissa e mobile.

12 MODALITA' GENERALI DI CONTROLLO

In base al principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, Statuto dei Lavoratori, come recentemente modificato dal D.Lgs. 151/2015 e dal D.Lgs. 185/2016). I dati devono essere gestiti soltanto dai soggetti preventivamente designati e autorizzati al loro trattamento, come da art. 2-quaterdecies del D.Lgs. 101/2018, secondo le modalità indicate nella Delibera Commissariale n. 936 del 30.11.2018.

Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzo non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Direzione Generale, attraverso gli Amministratori di Sistema, potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati non riconducibili al singolo utente, ma riferiti all'intera Struttura organizzativa o a sue articolazioni.

Il controllo sui dati anonimi si concluderà con una comunicazione al Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti aziendali, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento.

Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l’invito al personale afferente alla Struttura in cui è stata rilevata l’anomalia.

In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale. In nessun caso, ad eccezione di specifica richiesta da parte dell’Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

Oltre a ciò l’Azienda si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente ed in particolare, alle disposizioni in materia di proprietà intellettuale. Oltre a tali controlli di carattere generale, l’Azienda si riserva comunque

le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che abbiano causato danno all'amministrazione, che ledano diritti di terzi o che, comunque, risultino illegittime.

13 SANZIONI

Qualora i responsabili dei controlli rilevino degli utilizzi anomali delle risorse informatiche, telematiche e telefoniche, provvederanno tempestivamente ad informare il Direttore Amministrativo ed il dirigente della Struttura presso la quale l'utente presta la propria attività per gli opportuni e/o dovuti provvedimenti, eventualmente anche disciplinari, consequenziali.

14 REVISIONE E AGGIORNAMENTI

Tutti gli utenti possono sottoporre all'esame della Direzione Amministrativa eventuali proposte scritte per l'integrazione e/o la rettifica del presente documento. Il presente Regolamento è soggetto a revisione senza una frequenza minima e comunque su base di reale necessità o secondo l'evoluzione del Sistema Informatico e di telefonia dell' Azienda.

15 INFORMATIVA AI SENSI DELL' ART 13 REGOLAMENTO UE 679/2016

Il presente Regolamento costituisce informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e dell'art. 4 della Legge 20 maggio 1970 n. 300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.

L'Azienda assicura al presente Regolamento la più ampia diffusione presso gli utenti, mediante:

- pubblicazione nella intranet aziendale.
- comunicazione del testo a tutti i dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Azienda;
- consegna di copia del testo a tutti i futuri dipendenti e a coloro che a vario titolo presteranno servizio o attività per conto e nelle strutture dell'Azienda;

16 NORMATIVA DI RIFERIMENTO

- Indirizzi in materia di servizio di telefonia: Circolare del Ministero della Funzione Pubblica n. 6/96 del 13.03.96, la direttiva della PCM del 20.07.99 e la Direttiva del Ministero dell'Innovazione del 30.10.2001
- Direttiva n. 02/09 del 26/5/2009 del Dipartimento della Funzione Pubblica.

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati
- Provvedimenti del Garante per la protezione dei dati personali in materia di "Misure di Sicurezza", in particolare con riguardo agli amministratori di Sistema (Provvedimento generale del 27.11.2008);
- Decreto Legislativo 30/06/2003 n. 196 come modificato con D.Lgs. n. 101/2018;
- Decreto Legislativo 07/03/2005 n. 82 (c.d. "Codice dell'Amministrazione Digitale – C.A.D.");
- Legge 18/08/2000 n. 248 e Decreto Legislativo 29/12/1992 n. 518 (su Diritti d'autore)
- Provvedimento del Garante per la protezione dei dati personali del 01/03/2007, pubblicato sulla G.U.R.I. del 10/03/2007 n. 58, in cui sono indicate le regole per l'uso di Internet e della posta elettronica;
- D.P.R. 11/02/2005 n. 68 (G.U.R.I. del 28/04/2005 n. 97) che disciplina le modalità di utilizzo della P.E.C. non solo nei rapporti con la P.A., ma anche tra i privati cittadini;
- Decreto Ministeriale 02/11/2005 contenente le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata", pubblicato nella G.U.R.I. del 15/11/2005 n. 266;
- Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)".
- Legge n. 300/1970 (Statuto dei Lavoratori).